VŠB-TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Návrh a implementace lokální počítačové sítě v mateřské škole

Design and implementation of local area network in nursery school

Student: **Daniel Otisk**
Vedoucí bakalářské práce: **RNDr. Ivo Martiník, Ph.D.**

Ostrava 2013

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání bakalářské práce

Student: **Daniel Otisk**

Studijní program: B6209 Systémové inženýrství a informatika

Studijní obor: 6209R001 Aplikovaná informatika

Téma: Návrh a implementace lokální počítačové sítě v mateřské škole
Design and Implementation of Local Area Network in Nursery School

Zásady pro vypracování:

1. Úvod
2. Teoretická východiska v oblasti lokálních počítačových sítí
3. Analýza a popis současného stavu počítačové sítě
4. Návrh možného řešení k vytvoření počítačové sítě
5. Zhodnocení navrženého řešení a následná implementace
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků bakalářské práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

TANENBAUM, Andrew S. a David J. WETHERALL. *Computer Networks*. 5th ed. Boston: Prentice Hall, 2010. ISBN 978-0132126953.
HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.
KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **RNDr. Ivo Martiník, Ph.D.**

Datum zadání: 23.11.2012
Datum odevzdání: 10.05.2013

Ing. Petr Rozehnal, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

Prohlašuji, že jsem celou práci, včetně všech příloh, vypracoval samostatně. Přílohy č. 1, 2 a 3, dané mi k dispozici, jsem samostatně doplnil.

V Havířově dne 3. 5. 2013

.....

Daniel Otisk

Na tomto místě bych chtěl vyjádřit poděkování vedoucímu bakalářské práce RNDr. Ivu Martiníkovi, Ph.D. za odborné vedení a rady při zpracování. Také děkuji zástupkyni ředitele mateřské školy, ve které jsem návrh lokální sítě zpracovával, Leoně Draslíkové za konzultace, které mi velice pomohly při psaní této práce. Poděkování patří také mé rodině a přátelům za morální podporu.

Obsah

1 Úvod

Jako téma ke zpracování bakalářské práce jsem si zvolil „Návrh a implementace lokální počítačové sítě v mateřské škole“. Zvolil jsem si jej z důvodu, že je mi oblast počítačových sítí velmi blízká a našel jsem v ní zalíbení.

Pojem počítačové sítě je znám již mnoho let a sahá nejspíš až k počátku samotného Arpanetu. Postupem času se jako každá jiná technologie i počítačové sítě zdokonalují po všech směrech, Ať již hardwarově nebo softwarově. Nesmím opomenout, že také stoupá razantně kriminalita v IT a proto se musí sítě neustále zabezpečovat novými lepšími metodami. Čím „lepší“, větší nebo možná významnější subjekt jako obchodní společnost či firma, tím stoupá riziko různých napadání hackerů, zlodějů dat apod. V praxi to tedy znamená, že je zapotřebí v takových společnostech se proti nim určitým způsobem chránit. V některých případech, je to však i přes veškeré úsilí zabránit napadení zbytečné, neboť i např. společenství hackerů „Anonymouse“ se dokáže nabourat do systémů ministerstev nebo na servery Facebooku. To je však určitě jistým způsobem, v mém případě budování počítačové sítě do mateřské školy, extrém, který pravděpodobně nenastane.

V teoretické části a zároveň druhé kapitole této práce zdůrazním převážně základní informace v oblasti lokálních počítačových sítí. Mezi tyto informace patří, jaké má výhody počítačová síť a jaké jsou její základní prvky. Dále rozdělíme sítě podle několika hledisek a uvedeme některé modely sítí a také síťové protokoly. Zjistíme, co se skrývá pod pojmem strukturovaná kabeláž či IEEE 802 a stručně shrneme způsoby zabezpečení sítí. V dalších kapitolách (3., 4. a 5.) se zabývám hlavně praktickou částí a detailně rozebírám jednotlivé dílčí cíle této bakalářské práce.

Prvním cílem mé bakalářské práce je tedy analyzovat aktuální stav síťového propojení v jednotlivých místnostech v prostorách mateřské školy, jaký je v budově hardware, tedy kolik PC a jestli vůbec zvládnou práci v síti. Dále zda je v budově již nějaké síťové spojení s okolním světem, např. internetový modem apod.

Druhým dílčím cílem je navrhnout možné řešení k vytvoření kompletní sítě LAN vč. výběru případně nového síťového HW a SW, a to co možná nejlevněji. Ve většině případů by mohlo být v budově zřízeno bezdrátové spojení, v některých případech to však možná bude muset být řešeno kabelově. Tím mám na mysli mezi patry, případně větší vzdálenost mezi zdmi. Jelikož nejsem kompetentní jakožto technik, v úpravách a přizpůsobení budovy,

k protahování kabelů zdmi, instalaci síťových zásuvek apod., je na mě, abych vyhledal firmu, která tyto práce vykoná.

Třetím dílčím cílem práce je navrhnout konfiguraci sítě co se týče různých nastavení IP adres a podobných činností. K tomu mi dopomůže profesionální nástroj, aplikace od společnosti CISCO s názvem Packet Tracer, který umí síť virtuálně propojit a vyzkoušet případná nastavení, která budou vyhovovat mé konkrétní školní síti. S programem mám několik zkušeností, proto by mi mohl trochu usnadnit práci při vytváření sítě. Síť by měla splňovat základní požadavky, a to hlavně sdílení Internetu, případně pak souborů nebo tiskáren, přičemž nemusí dosahovat vysokých rychlostí přenosu dat.

Čtvrtý dílčí cíl práce se týká zabezpečení. Mateřská škola je docela malým terčem k vykonání nějaké kriminální činnosti. Proto zvolím jako zabezpečení bezdrátových sítí pouze přístupové heslo, případně filtraci fyzických MAC adres a dle potřeby sítě skryji pro veřejnost. Tyto zabezpečení je však potřeba při realizaci sítě operativně řešit s pracovníky školky dle jejich potřeb. Způsobilá osoba, zástupkyně ředitele, která mě při realizaci bude doprovázet, zatím není při začátku psaní této práce zcela rozhodnuta, zda bude síť přístupná např. rodičům jako přístup k Internetu apod. Zbytek sítě bude samozřejmě chráněn základním SW vybavením, firewallem a antivirem.

Posledním pátým dílčím cílem práce bude potom všechny tyto možnosti v návrzích finančně zanalyzovat a zhodnotit a předat tyto návrhy kompetentnímu pracovníku, v mém případě zástupkyni školy. Ta bude již potom rozhodující osobou, která se rozhodne o následujícím postupu k implementaci návrhů a celkové realizace sítě.

V poslední šesté kapitole, tedy závěru práce hodnotím jednotlivé dílčí cíle, bakalářskou práci jakožto celek a také její přínosy pro mě.

Práce je určena spíše pro mírně až středně pokročilé uživatele, neboť v rozsahu bakalářské práce není možné shrnout a vysvětlit všechny základní informace, které jsou nezbytné pro pochopení složitějších definicí či výrazů.

2 Teoretická východiska v oblasti lokálních počítačových sítí

V úvodu teoretické části bychom si měli uvést několik základních informací z této oblasti.

2.1 Výhody sítí

Shrňme si ve stručnosti, k čemu se sítě používají. Síť nám tedy umožňuje:

- sdílet data, která jsou pro více uživatelů důležitá,
- snadno přenášet data, bez používání disket, cd disků, flash pamětí apod.,
- sdílet hardwarové prostředky, jakými jsou například tiskárna, internetový modem nebo datový prostor na disku,
- komunikovat v síti, buďto interně mezi počítači nebo dnes již rozšířeně za pomocí Internetu,
- chránit data, která mohou být na jednom PC přístupná pro určité uživatele z různých míst v síti s různými omezeními. Snazší a levnější je také pravidelné zálohování dat. [2]

2.2 Základní prvky sítě

Co je tedy počítačová síť? Jde o souhrn hardwarových a softwarových prvků, které zprostředkovávají vzájemnou spolupráci počítačů. V našem praktickém případě v další kapitole potom půjde o lokální počítačovou síť tedy LAN (Local area network). [2]

2.2.1 Vybavení počítače

Samotný počítač by měl být vybaven programem, který umožňuje síťovou komunikaci. To však není problém, protože na většině počítačů jsou nainstalovány operační systémy Windows, které síťovou komunikaci umožňují zcela běžně. Hardwarovým prvkem, který by neměl pro úspěšnou komunikaci chybět, je síťová karta. Ta spojuje konkrétní počítač s jiným zařízením v síti, buďto za pomoci kabelů nebo bezdrátovým přístupem. [2]

2.2.2 Prvky sítě mimo PC

Síť je tedy propojena kabely a dalšími aktivními prvky jako je např. router (směrovač) nebo switch (přepínač). Tyto propojující prvky v síti potom zesilují či filtrují přenášená data apod. [2]

2.3 Dělení sítí

Sítě se dělí podle velkého množství kritérií, přičemž se kritéria vzájemně prolínají, síť tedy může vyhovovat více kritériím. Dělí se podle rozlehlosti, topologie, architektury, vlastnictví atd. Několik základních dělení si zde znázorníme.

2.3.1 Dělení sítí podle rozlehlosti

Zde není zcela přesná specifikace rozloh v měřitelných jednotkách a jednotlivé sítě se mohou mezi sebou kombinovat, ale můžeme je přesto rozdělit obecně aspoň jako:

- **PAN** – osobní síť (personal area network), která má vzdálenost řádově v několika pár metrech na dosah těla. Využívá se pro spojení např. mobilního telefonu, PDA, fotoaparátu. Technologie přenosu může být třeba bluetooth, infraport nebo za pomoci USB.
- **LAN** – lokální neboli místní síť (local area network) je omezena na jedno lokální místo, kde je tato síť umístěna např. v budovách, firmách, školách, domácnostech atd. a pro připojení se využívají většinou kabely. (HORÁK, 2011) V rámci jedné LAN se používá stejný linkový protokol (např. Ethernet). (DOSTÁLEK, 2008)
- **MAN** – metropolitní sítě (metropolitan area network) bývají mezi vzdálenějšími objekty (udává se zhruba do 75 km) např. v jednom městě. Obecně je větší než LAN, ale menší než WAN. Příkladem může být právě univerzitní síť mezi jednotlivými fakultami, rozmístěnými od sebe i v řádech kilometrů, a to kabely, ale i bezdrátově.
- **WAN** – rozlehlé globální sítě (wide area network) si představme jakožto více spojených sítí LAN a MAN. Mohou být i mezi celými státy, kontinenty atd. Hlavní příkladem je celosvětová síť Internet. (HORÁK, 2011)

2.3.2 Dělení sítí podle fyzických topologií

Tímto rozdělením udáváme fyzický způsob propojení jednotlivých stanic včetně instalovaných kabelů. Fyzická topologie je základním prvkem standardu sítě a podstatně určuje, jaké bude mít síť vlastnosti a kvality. (HORÁK, 2011)

Sběrnicová topologie (bus topology) – stanice jsou zde propojeny průběžně většinou koaxiálním kabelem. PC jsou spojeny se sítí pomocí odbočovacích prvků (např. T-konektorů). Výhodou je nízká spotřeba kabeláže, a tím pádem i nižší cena za propojení. Nevýhodou však je velký počet spojů v kabelu, což často zapříčiňuje mnoho poruch a potíží. Další nevýhodou je také fakt, že pokud se jakákoliv část v této síti poruší, tak zhavaruje celá síť a je obtížné tuto poruchu dohledat. (HORÁK, 2011)

Hvězdicová topologie (star topology) – jednotlivé stanice jsou propojeny v síti určitým středovým rozbočovacím zařízením, nejčastěji switchem nebo u starších sítí hubem. Ke každé stanici vede vlastní kabel, nejčastěji kroucená dvojlinka. Tato topologie je dnes nejčastějším případem. Velkou výhodou je malá náchylnost k chybě, a pokud přesto vznikne, je podstatně snazší ji lokalizovat než u sběrnicové topologie. (HORÁK, 2011)

Kruhová topologie (ring topology) – velmi podobná topologie jako sběrnicová s rozdílem, že jsou konce spojeny do souvislého kruhu. To umožňuje využívat metodu postupného předávání zpráv – token (viz dále). Nevýhoda je podobná jako u sběrnicové topologie, pokud se vyskytne porucha, vznikne většinou havárie celé sítě. To se však dá řešit zdvojením kabelů. (HORÁK, 2011)

Topologie sítí se mohou vzájemně kombinovat a různě na sebe navazovat. Takovým topologiím říkáme **hybridní** nebo též kombinované. Mohou být ale také **nesystematické**.

Existuje i dělení podle ***logických topologií***, kdy se ptáme na otázku, jak a kudy data prochází, přičemž data nemusí procházet tak, jak jsou fyzicky zapojena zařízení.

Příkladem jsou např. bezdrátové **ad-hoc** sítě, kdy se mezi sebou propojí dva až pět počítačů a jsou si mezi sebou rovny. Podstatnou výhodou takových sítí je rychlá a snadná instalace a velmi nízká cena pořízení, protože mimo klientské síťové adaptéry nepotřebujeme žádný další HW. Převážně síť umožňuje většinu běžných služeb jako v klasické síti LAN, jako je sdílení Internetu, souborů či tiskáren. Nevýhodou je však, že všechna zařízení musí být vzájemně v dosahu, musí na sebe vzájemně „vidět“. Dalším nebezpečím je díky snadné

instalaci také fakt, že se do sítě může také takto snadno kdokoliv dostat a je obtížné takovou síť zabezpečit. (DOSTÁLEK, 2008)

2.3.3 Dělení podle vlastnictví

Tímto kritériem se míní, pro koho je síť určena. Primárně se dělí na **veřejné** a **privátní**. Důležité je vždy hledisko využití sítě. Kdo je vlastníkem, provozovatelem a uživatelem nebo jaké služby síť poskytuje atd. U veřejných sítí provozovatel a vlastník není uživatelem, ale síť pronajímá dalším osobám většinou pro komerční využití. Typickým příkladem jsou páteřní sítě. Menší veřejné sítě bývají pak např. na letištích, ve školách, v kavárnách, případně v obchodních centrech apod. zejména k přístupu na Internet, ale i k využití jiných služeb. Privátní sítě jsou veškeré sítě, které nemáme v plánu zpřístupňovat cizím osobám a náležitě je proto proti cizímu vniknutí zabezpečujeme. Provozovatel, vlastník je zde také uživatelem, přičemž nemusí vlastnit celou síť. Využívají se v nich k identifikaci zařízení privátní IP adresy. Zdárným příkladem jsou sítě LAN, ať už v domácnostech, podnicích nebo např. na úřadech. [6]

Zvláštním typem tohoto rozdělení je i ***virtuální privátní síť*** (VPN). Jinými slovy je technicky vzato tato síť umístěna uvnitř nějaké jiné a je její součástí. Když na to přijde, tak smí být jeden článek fyzicky i 15 000 km vzdálený od zbytku sítě. Na venek se pro uživatele jeví jako samostatná. Tato síť má vlastní správu a vlastní pravidla. Z ekonomického hlediska je levnější variantou než budování „opravdové“ sítě. Vstup do ní je možný po autentizaci pomocí digitálních certifikátů a autorizaci a následně má uživatel umožněn volný pohyb, přičemž je síť sama o sobě odolná vůči okolnímu světu, a to především díky šifrování. (TANENBAUM, 2011)

2.4 Modely sítí

Základním kritériem, podle něhož rozdělujeme síťový SW, je použití (či nepoužití) serveru. Z tohoto hlediska rozeznáváme sítě peer-to-peer a klient-server. (HORÁK, 2011)

2.4.1 Síť typu peer-to-peer

V tomto typu sítě smí uživatel prostřednictvím své stanice komunikovat s jednou i více stanicemi v síti, přičemž se zde nerozlišuje, zdali je stanice klient nebo server. Teoreticky se můžete spojit s jakýmkoli zařízením v síti. Mnoho peer-to-peer, též P2P, sítí, jako je BitTorrent, nemají centrální databázi s uloženými daty. Namísto toho má každý uživatel vlastní databázi na svém lokálním PC a může ji nabízet ostatním členům sítě. Každý nový uživatel smí vidět u existujících členů, jaká vlastní data a také jména dalších členů, s kterými je spojen, a taktéž posléze sdílet popř. stahovat jejich data. Tímto opakujícím se procesem jsme schopni vybudovat opravdu velkou lokální databázi. (TANENBAUM, 2011)

P2P komunikace jsou často využívány ke sdílení hudby a videí. Velmi významným „boom“ okamžikem byl okolo roku 2000 sdílení hudby prostřednictvím služby Napster, který byla však ukončena, protože nesplňovala legální požadavky, co se týče autorství apod. Existují však také legální P2P sítě. Smíte prostřednictvím nich sdílet např. svou produkci hudby, rodinné fotografie či videa nebo např. volně šiřitelný software. Na podobném principu, jako jsou tyto sítě, pracuje komunikační služba email. Tato služba je mezi lidmi oblíbená již řadu let a pravděpodobně ještě dlouho bude. (TANENBAUM, 2011)

2.4.2 Síť typu klient-server

V tomto modelu sítě jsou data uloženy především na výkonnějších počítačích, kterým říkáme servery. Ty jsou většinou spravovány různými administrátory a správci. Zbývající prvky sítě jsou tzv. „klienti“, ve firmě to jsou hlavně pracovní stanice zaměstnanců. Ty mají menší nároky na výkon. Klientské počítače a servery jsou mezi sebou propojeny sítí. (TANENBAUM, 2011)

Tento model je rozšířenější a má lepší využití než u P2P sítí. Nejpopulárnějšími službami, které tento model poskytuje, jsou webové aplikace. Ty jsou poskytovány prostřednictvím webových stránek, které jsou uloženy právě na serverech. Tento model smí být aplikován v rámci jedné budovy či firmy, samozřejmostí je však i to, že se k serveru dostanete např. i prostřednictvím sítě tzv. „z venku“. (TANENBAUM, 2011)

2.5 Síťové protokoly

Síťové protokoly slouží ke komunikaci počítačů v počítačové síti. Existuje jich celá řada. V Internetu a také u sítí LAN se používají především protokoly TCP/IP. (DOSTÁLEK, 2008)

Síťový protokol je *norma* nebo též *standard*. V Internetu se používají normy (resp. závazná doporučení) nazývané Request For Comments (RFC), které jsou číslovány od jedničky. V současné době jich je přes pět tisíc, ale ne všechny se dnes již používají. Tyto normy jsou volně ke stažení na Internetu (viz www.rfc-editor.org). (DOSTÁLEK, 2008)

Vedle norem RFC se vyskytují také jiné normy, které však vydaly jiné organizace:

- ISO (International Organization for Standardization). Normy této organizace jsou volně dostupné např. v informačním středisku Českého normalizačního institutu se sídlem v Praze.
- ITU (International Telecommunication Unin). Je jednou z nejstarších celosvětových organizací vůbec se sídlem v Ženevě. Byla založena roku 1865. Její normy jsou dostupné k prostudování v knihovně ústavu TESTCOM (Technický a zkušební ústav telekomunikací a pošt, se sídlem v Praze). (DOSTÁLEK, 2008)

Na jiných vrstvách vrstveného modelu TCP/IP (viz níže) se pak dále setkáme s americkými normami:

- IEEE – profesní organizace zabývající se pokročilými technologiemi. Mezi její nejznámější normy patří řada norem IEEE 802, které jsou mj. také dostupné na Internetu. Tyto normy se od sebe odlišují v názvu, a to tak, že za číslem 802 následuje tečka a za ní další číslo, jako např. 802.11, což je standard pro Wi-Fi (viz dále). K této normě se pojí řada dalších dodatků, jako např. 802.11g, 802.11n apod., které označují specifické vlastnosti normy, jako je v tomto případě např. rychlost přenosu dat atd.
- TIA (Telecommunications Industry Association) – asociace amerických společností zabývající se telekomunikacemi.
- EIA (Electronic Industries Aliance) – asociace amerických výrobců elektroniky. (DOSTÁLEK, 2008)

Celá problematika síťových komunikací je poměrně komplikovaná, proto je potřeba ji rozdělit do několika vrstev. Počet vrstev záleží na soustavě protokolů, které při síťové komunikaci využíváme. Nejčastěji se setkáme se soustavou protokolů, které se nachází na Internetu, a tím mám na mysli rodinu protokolů TCP/IP, která je čtyřvrstvá. Existuje však také jiné rozdělení do vrstev, a to podle modelu ISO/OSI, kterou vytvořila zmiňovaná organizace ISO. Tato soustava je sedmivrstvá, je dokonale propracovaná a jednu dobu se dokonce zdálo, že odsune do pozadí i soustavu TCP/IP. (DOSTÁLEK, 2008)

Jednotlivé vrstvy a jejich stručný popis zobrazuje následující tabulka 2.1.

Tabulka 2.1: Úkoly vrstev modelu ISO/OSI

Vrstva	**Popis**
Fyzická vrstva (Physical Layer)	Týká se přenosu neinterpretovaných bitů přes komunikační kanál. (TANENBAUM, 2010) Popisuje elektrické (či optické), mechanické a funkční vlastnosti: jakým signálem je reprezentována logická jednička, jak přijímací stanice rozezná začátek bitu, jaký je tvar konektoru, k čemu je který vodič kabelu použit atd. (HORÁK, 2011, str. 24)
Linková (spojová) vrstva (Data-link Layer)	Hlavní úlohou této vrstvy je odhalování a oznamování detekovaných chyb a jejich korekce. (TANENBAUM, 2010) Uskutečňuje přenos údajů (datových rámců) po fyzickém médiu, pracuje s fyzickými (MAC) adresami síťových karet, odesílá a přijímá rámce, kontroluje cílové adresy každého přijatého rámce, určuje, zda bude rámec odevzdán vyšší vrstvě atd. (HORÁK, 2011, str. 24)
Síťová vrstva (Network Layer)	Je zodpovědná za spojení a směrování mezi dvěma počítači nebo celými sítěmi (tj. uzly), mezi nimiž neexistuje přímé spojení. Zajišťuje např. volbu trasy při spojení (mezi uzly bývá více možných cest pro přenos paketu). (HORÁK, 2011, str. 24) Na této vrstvě pracují zařízení, jako je router. (TANENBAUM, 2010)
Transportní vrstva (Transport Layer)	Typickou činností transportní vrstvy je dělení zprávy (segmentu) na pakety a opětovné skládání přijatých paketů do zpráv (při přenosu se mohou pakety pomíchat či ztratit). (HORÁK, 2011, str. 24) Na této vrstvě pracují protokoly TCP a UDP. (TANENBAUM, 2010)

Relační vrstva (Session Layer)	Navazuje a po skončení přenosu ukončuje spojení, tzv. relace. Nabízí různé služby, jako jsou: řízení dialogů a tzv. tokenů, ověřování uživatelů, zabezpečení přístupu k zařízením, synchronizace atd. (TANENBAUM, 2010)
Prezentační vrstva (Presentation Layer)	Má na starosti konverzi dat, přenášená data mohou být totiž v různých sítích různě kódována. Sjednocuje formy vzájemně přenášených údajů. Dále může data komprimovat, případně šifrovat. V praxi často splývá s relační vrstvou. (HORÁK, 2011, str. 24)
Aplikační vrstva (Application Layer)	Obsahuje sadu protokolů, které většinou potřebují uživatelé k vykonání určité aplikace. Jeden z nejrozšířenějších protokolů je HTTP (HyperText Transfer Protocol), který je základem pro WWW (World Wide Web). Vrstva je potřebná pro řadu aplikací, jako jsou webové prohlížeče, emailoví klienti, FTP klienti, RSS kanály apod. (TANENBAUM, 2010)

Tyto dvě soustavy protokolů se od sebe liší a jsou vzájemně neporovnatelné. Z obrázku 2.1 je však patrné, že si jsou vrstvy mezi sebou velmi blízké. Rodina síťových protokolů TCP/IP neřeší (až na výjimky) fyzickou a linkovou vrstvu, kde se jim říká vrstva síťového rozhraní, a proto se na Internetu setkáváme s těmito vrstvami z modelu ISO/OSI. (DOSTÁLEK, 2008)

Obrázek 2.1: Srovnání modelu TCP/IP s modelem ISO/OSI (zdroj: wikipedia.org)

2.5.1 Protokol TCP/IP

Jde o nejrozšířenější skupinu protokolů, která byla původně navržena pro síť, z níž se postupem času vyvinul Internet. V dnešní době je tato sada protokolů využívána primárně v sítích LAN, kde se stala standardem a své předchůdce z této pozice vytlačila. (HORÁK, 2011)

Co se týče funkčního hlediska, můžeme soubor protokolů TCP/IP rozdělit do tří vrstev, které jsou reprezentovány vlastními protokoly:

- aplikační vrstvu (spolupracující s jednotlivými programy, viz tab. 2.2),
- transportní vrstvu (protokoly TCP a UDP),
- síťovou vrstvu (protokoly IP). (HORÁK, 2011)

Spolupráce vrstev probíhá přibližně zjednodušeně takto: „Program (tj. aplikace) potřebuje navázat spojení se svým protějškem na jiném počítači. Použije k tomu aplikační vrstvu, od níž putuje požadavek na spojení do transportní vrstvy. Ta zorganizuje dopravu dat (data rozdělí na segmenty, naváže spojení, zkontroluje, zda byla data doručena). Vlastní přenos zajišťuje nižší – síťová vrstva. Segmenty, které obdržela od nadřazené vrstvy, „zabalí“ do datagramů a doručí vzdálenému počítači.“ (HORÁK, 2011, str. 76)

2.5.1.1 Aplikační vrstva

Je tvořena množinou protokolů, které spolupracují s jednotlivými aplikačními programy. Uživatelé se přes internetové prohlížeče (dnes vyhrává Google Chrome, dále Mozilla Firefox, Opera, Internet Explorer nebo v neposlední řadě Safari od spol. Apple), dostanou k webovým stránkám, které jsou uloženy na webových serverech. Stránky jsou uživatelům nabízeny různými speciálními programy pro publikace WWW, ale tuto činnost dokáže zprostředkovat i samotný operační systém MS Windows. Zde můžeme vidět, že při surfování po Internetu spolupracují různé programy různých výrobců. Celou spolupráci zajišťují právě aplikační protokol, neboli soustava již zmiňovaných norem, které musí tyto programy respektovat. Konkrétně při prohlížení webových stránek jím je protokol HTTP. (HORÁK, 2011)

Aplikačních protokolů existuje mnoho a některé z těch důležitých si znázorníme v následující tabulce 2.2.

Tabulka 2.2: Nejznámější aplikační protokoly (HORÁK, 2011, str. 77)

Služba	**Funkce**
FTP – File Transfer Protocol (datový kanál)	Používá se pro přenos souborů mezi vzdálenými PC
Telnet	Pro jednoduché terminálové relace (v podstatě ovládáme obrazovku vzdáleného PC)
Server DNS – Domain Name Systém	Organizuje názvy počítačů v Internetu a jejich vazby na IP adresy
WWW – protocol HTTP (Hypertext Transfer Protocol)	Protokol používaný k uspořádání WWW stránek a pohybu mezi nimi
SMTP – Simple Mail Transfer Protocol	Protokol zajišťující přenos zpráv mezi servery Internetu (používaný hlavně pro elektronickou poštu)
POP3 – Post Office Protocol	Jeho posláním je dopravit poštu z elektronické schránky na náš počítač

2.5.1.2 Transportní vrstva

V soustavě TCP/IP je tato vrstva pomyslným jádrem, které tvoří pouze dva protokoly a to *TCP (Transmission Control Protocol)* a *UDP (User Datagram Protocol)*. UDP na rozdíl od TCP nepotřebuje vytvářet před přenosem dat relaci s protějškem a nekontroluje ani, zda byly data druhou stranou přijaty. Protokol UDP je tedy jednodušší, ale tím i méně spolehlivý. Výhodný je pouze pro svůj rychlý přenos, využívá se tedy tam, kde není zapotřebí spolehlivá komunikace. (HORÁK, 2011)

2.5.1.3 Síťová vrstva

Dále zde existuje protokol *IP (Internet Protocol)*, který pracuje v síťové vrstvě rodiny TCP/IP. Ten přidává k jednotlivým segmentům dat vlastní hlavičku a vytváří tím datagram IP. V hlavičce je udána IP adresa příjemce a odesílatele zprávy, což je velmi důležité pro doručení jednotlivých datagramů k příjemci. Tomuto postupu se říká adresování a směrování mezi počítači. (HORÁK, 2011)

Protokol IP je nespojovaný, tzn., že před zahájením výměny dat nevytváří žádnou relaci. Dále je nespolehlivý, což znamená, že po výměně dat není provedena kontrola úspěšného doručení. Pakety IP se mohou z tohoto důvodu ztrácet, mohou být doručeny

v jiném pořadí, mohou být zdvojeny nebo zpožděny. Protokol IP sám o sobě tyto chyby neopravuje. Tento problém řeší nadřazená transportní vrstva, konkrétně protokol TCP. (HORÁK, 2011)

2.5.1.3.1 Adresace v sítích TCP/IP

Adresace je prakticky nejdůležitější činnost při zprovozňování počítačové sítě založené na protokolu TCP/IP. (HORÁK, 2011)

Základním aspektem pro adresaci jednotlivých stanic je to, aby měla každá stanice své originální číslo a zřejmé označení konkrétní sítě, či segmentace v síti. Každá stanice má tedy svou IP adresu, která je sestavena čtveřicí čísel oddělených tečkami, např. takto 192.168.1.11. V příkladu je konkrétně znázorněna adresa v nejpoužívanější desítkové soustavě, adresace však může být převedena i do dvojkové, která vypadá takto: 11000000.10101000.00000001.00001011, nebo do šestnáctkové soustavy takto: C0.A8.01.11. Dvojková soustava má pouze dva prvky a to 0 a 1 a využívají jí především hardwarové prvky PC. Šestnáctková neboli hexadecimální soustava má šestnáct znaků a to 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. S ní se však v adresaci IP setkáme jen zřídka. (HORÁK, 2011)

Protože se stanice nacházejí v různých sítích, které mezi sebou spolupracují, nestačí uvést pouze číslo konkrétního počítače, ale potřebujeme znát ještě číslo sítě nebo jejího segmentu (podsítě), ve které je PC zařazen. IP adresa se tedy dělí, jak jsme již načali, na hostitelskou a síťovou část. Podle toho, jaká část je věnována síti a jaká číslu PC, jsou adresy roztříděny do jednotlivých tříd. (HORÁK, 2011)

Jak můžeme dále v tabulce 2.3 vidět, je IP adresa u tříd A, B a C navržena variabilně. Adrese sítě je možné vyhradit 1 až 3 číslice (bajty), zbytek adresy je tedy hostitelská část neboli adresa uzlu. (HORÁK, 2011)

Tabulka 2.3: Třídy sítí IP (zdroj: [1], [2])

	Rozsah adres prvního číslo	Počet čísel vyhrazených pro adresu sítě	Počet čísel vyhrazených pro adresu uzlu	Využití
Třída A	0-127	1 (adresuje 126 sítí)	3 (adresuje asi 17 mil. uzlů = PC)	Pro rozsáhlé sítě
Třída B	128-191	2 (adresuje 16 tis. sítí)	2 (adresuje asi 65 tis. uzlů)	Středně velké sítě
Třída C	192-223	3 (adresuje 2 mil. sítí)	1 (adresuje asi 254 uzlů)	Menší sítě (např. LAN)
Třída D	224-239	-	-	Multicastové adresy
Třída E	240-255	-	-	Vyhrazeno pro budoucí využití

IP adresy se začali využívat dříve v Internetu, potom až v lokálních sítích. Z důvodu aby nedocházelo ke konfliktům a střetům mezi IP adresami lokálu a na Internetu, vymezily se pro lokální sítě adresové rozsahy. Jsou to:

- Třída A: 10.0.0.0 až 10.255.255.255.
- Třída B: 172.16.0.0 až 172.31.255.255.
- Třída C: 192.168.0.0 až 192.168.255.255. (HORÁK, 2011)

Zároveň pro poznání síťové a hostitelské části v IP adrese nám slouží tzv. *maska sítě*. Ta je taktéž čtyřbajtová a vychází přirozeně z dvojkové soustavy. Část, která tvoří tu síťovou je označena většinou primárně osmi jedničkami. Zvlášť pro IP adresy, které jsou vyhrazeny pro lokální sítě, se používají standardní síťové masky:

- pro **třídu A** je dvojkový tvar 11111111.0000000.00000000.00000000, pro hexadecimální FF.00.00.00 a pro desítkový 255.0.0.0,
- pro **třídu B** je to dvojkový tvar 1111111.1111111.0000000.00000000, šestnáctkový FF.FF.00.00 a decimální 255.255.0.0,
- pro **třídu C** to jsou tvary 11111111.11111111.11111111.00000000, FF.FF.FF.00 a 255.255.255.0.

V ukázkách vidíme, že pro síťovou masku třídy A je vyhrazen první bajt, pro třídu B dva bajty a pro třídu C tři bajty. (HORÁK, 2011)

O IP adresách třídy D a E se v terminologii lokálních sítích zatím moc nemluví. Třída D však začíná v posledních letech sloužit na Internetu pro multicastové vysílání. V minulosti se *multicast* téměř nevyužíval. Do této třídy spadá pár adres se speciálním účelem. Například nejnižší adresa 0.0.0.0 je využita pro hosty, kteří se v daném okamžiku připojují (bootují). Naopak nejvyšší adresa 255.255.255.255 pak označuje všechny hostující zařízení v uvedené síti, řečeno jinak také *broadcast* nebo broadcastové rozesílání paketů. Tuto možnost však spoustu síťových administrátorů ve své síti zakazuje, neboť je to docela bezpečnostní hazard. (TANENBAUM, 2010)

Mezi další speciální adresy, které jsou vyhrazené pro určité objekty, patří i IP adresy začínající číslem 127.x.x.x, např. 127.0.0.1, která neodmyslitelně testuje funkčnost každé jednotlivé stanice (hosta) respektive síťové karty, jinak řečeno také *loopback*. Tato možnost povoluje odesílat pakety bez adresy příjemce pouze však na lokální stanici. (TANENBAUM, 2010)

2.5.1.3.2 Propojování sítí TCP/IP

Ve většině případů je zapotřebí propojit počítače z jedné organizované sítě do nějaké jiné. Proto je nastavení každého počítače další údaj, a to výchozí brána neboli anglicky gateway. Tato část je u nastavení nepovinná, nýbrž pro správný přístup k jiné síti nezbytný. Prakticky je tato výchozí brána další IP adresou, která označuje zařízení jako např. router (směrovač), ale může to být i další PC s dvěma a více síťovými kartami, který nám přístup do dalších sítí umožnuje. Pokud je tedy v požadavku na komunikaci jiná IP adresa, než je rozsah adres ve vlastní lokální síti, je tento požadavek směrován k bráně, který jej předává dál do správných míst. (HORÁK, 2011)

2.5.2 DHCP (Dynamic Host Configuration Protocol)

Při vytváření sítě a přidělování IP adres jednotlivým stanicím využíváme dvou způsobů přidělení:

- **Staticky**, kdy přidělujeme adresu ručně a trvale.
- **Dynamicky**, kdy se adresy přidělují automaticky na určitou dobu za pomoci DHCP protokolu. (DOSTÁLEK, 2008)

Pokud si zvolíme druhou možnost a nechceme IP adresy pracně přidělovat ručně, musí v síti existovat tzv. DHCP server s příslušným nastavením. Při spuštění počítače, který se snaží přihlásit k síti, dochází k požadavku, kterému se říká tzv. DHCP Discover paket, který je odeslán právě k DHCP serveru. Pokud v místní síti není žádný DHCP server v dosahu, tak směrovač (router) je proto nakonfigurován k odeslání DHCP broadcastu (zaslání každému zařízení v síti, i dalšímu routeru), dokud není tento server nalezen. V okamžiku, kdy server obdrží požadavek, alokuje volnou IP adresu vhodnou pro danou síť a pošle ji stanici jakožto DHCP Offer paket. (TANENBAUM, 2011)

DHCP server může běžet na platformách UNIX, Windows Server atp. Dále může být realizován jako součást routeru, switche nebo přístupového bodu WiFi sítě (též AP). (DOSTÁLEK, 2008)

Dynamické přidělování IP adres je také výhodné v tom, že je zapotřebí vždy jen tolik IP adres, kolik je přihlášených uživatelů. Tento způsob přidělování dnes řeší aplikační protokol DHCP, který vychází ze zkušeností a částečně v sobě obsahuje i podporu starších protokolů, které se tohoto přidělování týkají. Jsou to např. RARP, DRARP a BOOTP. (DOSTÁLEK, 2008)

2.5.3 DNS (Domain Name System)

Služba, která byla vyvinuta pro Internet, kde také později jako v lokálních sítích, musí mít každá stanice svou IP adresu a bylo velmi obtížné si všechny tyto adresy zapamatovat. Z tohoto důvodu existuje systém DNS, který převádí čísla na lépe zapamatovatelné názvy. Všechny počítače jsou rozděleny pomoci DNS do zón – domén, které se dále řadí do stromové struktury a společně mezi sebou dle potřeby komunikují. Např. všechny počítače v České Republice mají doménu .cz. Doména se zadává pouze v případě, pokud chceme počítač připojit k síti Internet a je zapotřebí zadat do nastavení alespoň jednu adresu serveru DNS, který už se stará o zbytek této práce. (HORÁK, 2011)

2.5.4 Fyzická adresa (MAC)

Jak jsme se již zmínili, IP adresy ale i IP pakety fungují na síťové vrstvě TCP/IP modelu. Rámce a fyzické adresy však fungují na vrstvě linkové. Prakticky jde o fyzickou neboli MAC adresu síťové karty, přičemž opět tato adresa je v síti unikátní. Nelze změnit, je

zadána již při její výrobě. Tyto adresy jsou šestibajtové, s tím, že první tři bajty udávají výrobce, který má své číslo již přiděleno a zbývající tři bajty identifikují danou síťovou kartu. (HORÁK, 2011)

2.6 Strukturovaná kabeláž

Víme, že pro stavbu sítě smíme využívat různé typy kabelů, kterými můžeme vytvářet různé topologie sítí. Co se týče rozvržení hardwaru a jeho uspořádání v sítí je nejspíš optimální řešení tzv. strukturovaná kabeláž. Základem je hvězdicová topologie, která je založena na kroucených dvojlinkách. Propojení se realizuje pomocí zásuvek, které mají každá svůj kabel. Zásuvky mají většinou dvě zdířky pro připojení dvou zařízení (PC, telefon, fax, tiskárna atd.). Dále se zde využívají rozvaděčové skříně (tzv. racky), kde jsou umístěny řídící přístroje jako např. switch nebo telefonní ústředna. Obvykle se umísťuje tato skříň na patro v budově a každá místnost má svou zásuvku. Využití této technologie má několik výhod:

- Umožňuje využít zásuvky jak datově, tak pro telefonní přenosy.
- Hvězdicová topologie usnadňuje údržbu a rychlejší vyhledání poruchy.
- Ochrana investic – sice jsou vyšší počáteční investice, ale na druhou stranu je později možné za minimální náklady různě rozšiřovat, měnit konfigurace nebo celé komunikační prvky velmi jednoduše. (HORÁK, 2011)

2.6.1 Aktivní prvky kabeláže

Nejjednodušším používaným zařízením je pravděpodobně zesilovač, nebo také opakovač či anglicky **repeater**. Ten má za úkol pouze zesílit signál, který jim prochází, aby se dosáhlo větší vzdálenosti mezi dvěma prvky. (HORÁK, 2011)

Hub je jednoduše rozbočovač, který pouze opakuje signál a šíří ho do všech připojených kabelů. Huby se již dnes nevyužívají, ale stále je v některých sítích nalezneme. (HORÁK, 2011)

Dalším dnes již standardním zařízením je **switch** nebo také přepínač. Ten čte pakety, které k němu dorazí a zasílá je pouze do větve, kde se nachází cílové zařízení. Pakety jdou tedy pouze na rozdíl od hubu od počátečního zařízení do koncového. Switch funguje plně duplexním přenosem dat (oběma směry zároveň), přičemž může komunikovat více dvojic

zařízení. Existuje ve dvou podobách, buďto jako stolní zařízení nebo již zmíněný rack, který se vkládá do rozvaděčové skříně. (HORÁK, 2011)

Prozatím nejinteligentnějším zařízením v síti je **router** neboli směrovač. Toto zařízení, pracující na síťové vrstvě modelu ISO/OSI, má za úkol shromažďovat informace o připojených sítích (využívá k tomu tabulku adres) a vybírat optimální cestu pro zasílané pakety mezi jednotlivými sítěmi. Často se využívá k připojení k Internetu, protože v sobě může mít zabudovanou např. filtraci paketů. (HORÁK, 2011)

Posledním námi zmíněným zařízením je **brána** (gateway), která pracuje na aplikační vrstvě modelu ISO/OSI a slouží k připojování LAN sítí k cizímu prostředí. Bránou může být považována právě i router, který je spojen s přívodem sítě Internet. (HORÁK, 2011)

V následující tabulce 2.4 stručně shrneme zmíněné aktivní prvky.

Tabulka 2.4: Rychlý přehled aktivních prvků s odpovídající vrstvou modelu ISO/OSI (HORÁK, 2011)

Aktivní prvek	Funkce	Vrstva ISO/OSI
zesilovač	zesiluje signály	fyzická
rozbočovač	rozvádí signály do všech větví sítě	fyzická
switch	filtruje pakety, propojuje pouze komunikující stanice	linková
směrovač	směruje pakety	síťová
brána	propojuje dvě rozdílné sítě	aplikační

2.7 IEEE 802

„IEEE 802 je rodina standardů pro lokální sítě (LAN), metropolitní sítě (MAN), i osobní sítě (PAN).“ (DOSTÁLEK, 2008, str. 64) Standardy spadají pod fyzickou i linkovou vrstvu, přičemž u linkové vrstvy se dělí ještě na několik podvrstev. Tzv. „horní patra“ tzn. 802.1 a 802.2 jsou společná pro všechny protokoly pod nimi. (DOSTÁLEK, 2008)

V rodině protokolů IEEE 802.2 existují podskupiny protokolů, mezi něž patří:

- „Skupina IEEE 802.3, která specifikuje Ethernet. Tyto protokoly se oficiálně nazývají CSMA/CD podle mechanismu přístupu k přenosovému médiu.
- Skupina IEEE 802.11, která specifikuje bezdrátové lokální sítě (WLAN) v nelicencovaných pásmech.
- Skupina 802.15 pro osobní sítě (PAN).“ (DOSTÁLEK, 2008, str. 65)

2.7.1 Ethernet

Ethernet je protokol vyvinutý společností DEC, Intel a Xerox (první označení Ethernet II) s přenosovou rychlostí 10 Mb/s. Organizace IEEE později označila protokol Ethernet pod označením 802.3. Oficiálně ho však nyní nenazývá jako Ethernet, ale CSMA/CD. Značení podle mechanismu přístupu k přenosovému médiu. (DOSTÁLEK, 2008)

V této části se Dostálek (2008) zmiňuje také k tomu, že je názorné říci vyjádření, že lokální sítě jsou jako sběrnice, přičemž sběrnici můžeme vnímat jako koaxiální kabely. (DOSTÁLEK, 2008) Zde zmiňuje ale i Horák, že se jedná hlavně o normy 10BASE-5 a 10BASE-2. (HORÁK, 2011) Ty byly společným médiem pro přenos informací. Na společném médiu se pro výměnu rámců mezi stanicemi používal *protokol CSMA/CD*, přičemž jsou si všechny stanice na společném médiu rovny. „Potřebuje-li nějaká stanice vysílat, poslechne si, zdali jiná stanice právě nevysílá. V případě, že médium není používáno (jiná stanice nevysílá), může stanice začít vysílat. Tento postup se nazývá Carrier Sense Multiple Access – CSMA.“ (DOSTÁLEK, 2008, str. 66) Zkratka CD (Collision Detection) je označení postupu, který zamezuje kolizím. (DOSTÁLEK, 2008)

V souvislosti s Ethernetem je třeba již teď zmínit, že kvůli omezené délce koaxiálního kabelu (několik set metrů), bylo potřeba využívat různých opakovačů (repeaterů) a později i přepínačů (switchů) či méně využitelných mostů (bridgů), aby se prodloužila vzdálenost. Pomalu se začalo upouštět od koaxiálních kabelů a přešlo se ke krouceným dvojlinkám s menšími vzdálenostmi a na páry optických vláken pro větší vzdálenosti. (DOSTÁLEK, 2008) Opět Horák zmiňuje, že se jedná především o normu 10BASE-T. (HORÁK, 2011) Pro stabilně vyšší rychlosti přenosu pak využíváme tzv. plně duplexní provoz (full duplex), kde je odděleno vysílání od příjmu. (DOSTÁLEK, 2008)

2.7.1.1 Fast Ethernet

Tato norma, odpovídající doporučení 802.3, je v dnešní době nejrozšířenější. Jedná se o metodu datových přenosů založené na přístupu CSMA/CD a dalších dílčích pravidlech. Zde

na rozdíl od klasického Ethernetu s rychlostí 10 Mb/s není možné využívat koaxiálních kabelů, na druhou stranu je přenosová rychlost navýšena na 100 Mb/s. Značí se také jako 100BASE-T a využívá se tedy převážně kroucené dvojlinky kategorie 5 (vzdálenost mezi 2 zařízeními maximálně 100 m), starší typy i kategorie 3 a 4, nebo optických vláken, kde může být délka segmentu až 412 metrů pro vícevidové kabely a poloviční duplex nebo až 10 000 m pro jednovidový kabel a full duplexní režim. (HORÁK, 2011)

2.7.1.2 Rychlejší typy Ethernetu

Existuje také tzv. gigabitový Ethernet, což je nejnovější variací Ethernetu, kdy se dosahuje rychlostí až 1 000 Mb/s a je také standardizovaný pro optické kabely a kroucenou dvojlinku. Značí se také jako 1000Base-X s podnormou 802.3z pro optické kabely a 1000Base-T s podčástí normy 802.3ab pro kovové kabely. Vzdálenost přenosu je pro mnohovidové optické kabely až 550 m a pro jednovidové až 5 km. (HORÁK, 2011)

Ještě se musíme zmínit také o verzi 10GB Ethernetu s normou 802.3ae, která je nyní nejrychlejším Ethernetem pro sítě LAN, ale je použitelná i pro MAN a WAN sítě. To je podpořeno právě vzdáleností, na které se dají sítě s tímto Ethernetem skládat, a to až 40 km s jednovidovými optickými vlákny. Je možnost na kratší vzdálenost i mnohovidové vlákna, ale to je prozatím vše. Metalické normy 10GB Ethernetu jsou ale již ve vývoji. (HORÁK, 2011)

2.7.2 Bezdrátové lokální sítě WLAN

Bezdrátové lokální sítě (Wireless Local Area Network) WLAN, taktéž značené jako WiFi nebo Wi-Fi, jsou v dnešní době velice oblíbené, a to zejména pro své výhody jako jsou:

- mobilita – nejsme vázaní kabeláží,
- rychlost a jednoduché zprovoznění,
- nízké náklady na vybudování sítě,
- jsou kdykoliv jednoduše rozšiřitelné,
- roaming – pokud je nastaven, mohou se mobilní stanice pohybovat volně po rozsahu dostupnosti sítě, přičemž se automaticky přepojuje k jiným přístupovým bodům (též AP bodům). (DOSTÁLEK, 2008)

Wi-Fi sítě se běžně využívají ve vnitřních i vnějších prostorách. Mohou být v kombinaci se strukturovanou kabeláží, kdy pevné stanice jsou připojeny kabely a přenosná

zařízení bezdrátově. Jsou velmi výhodné pro dočasné využívání sítě a jsou vhodné pro různá výstaviště, studentské koleje, ale i v objektech samotných škol. (DOSTÁLEK, 2008)

Přenosové médium je pro bezdrátové sítě rádiové vysílání o kmitočtu 2,4 GHz (v ČR je v tomto pásmu možno využít 14 kanálů – 0 až 13) nebo 5 GHz. U nás však 5 GHz WLAN není povolena. V sítích je kvůli nepovinnosti licencování u Českého telekomunikačního úřadu možné i rušení, protože se mohou sítě navzájem střetávat. (DOSTÁLEK, 2008)

WLAN specifikuje norma IEEE 802.11 a používá protokol přístupu k médiu nazývaný CSMA/CA. Je odvozen od CSMA/CD jako u Ethernetu, ale na rozdíl od něj je u bezdrátového vysílače těžké detekovat kolize, proto se k jejich detekci využívá systém potvrzování. (DOSTÁLEK, 2008)

Norma 802.11 se stále rozšiřuje, z důvodu stálého vylepšování funkcí. Mezi takové rozšíření patří zejména 802.11b a 802.11g. (DOSTÁLEK, 2008) Norma 802.11n, která je prozatím nejnovější pracuje takovým způsobem, že zařízení vysílá několik signálů různými cestami prostřednictvím více antén. (HORÁK, 2011) V tabulce 2.5 vidíme stručné shrnutí.

Tabulka 2.5: Základní vlastnosti bezdrátových standardů (HORÁK, 2011)

Standard	Pásmo	Teoretická max. rychlost [Mb/s]	Dosah
802.11a	5	54	50
802.11b	2.4	11	100
802.11g	2.4	54	100
802.11n	2,4 nebo 5	600	250

2.7.2.1 Bezpečnost

Zabezpečit bezdrátovou síť je oproti zabezpečování metalických sítí mnohem složitější, protože při jejím provozu je základním problémem, že se rádiový signál šíří všemi směry a může ho tedy kdokoliv odposlouchávat nebo se do sítě nějakým způsobem zapojit. Bezpečnost je tedy u těchto sítí opravdu na místě a neměla by se zanedbávat. Mezi zásadní bezpečnostní opatření patří tyto dvě:

- **Autentizace** – kontrola oprávněnosti při přiřazování nové stanice do bezdrátové sítě (zabezpečení proti „cizincům“).
- **Kódování** – přenášená data jsou šifrována a to tak, aby se nedala vyluštit ani po jejich zachycení. (HORÁK, 2011)

Ochranných metod máme hned několik. Ty se postupně zdokonalují a zařazují mezi standardy Wi-Fi. Dle bezpečnostních metod můžeme určit kvalitu hardwaru Wi-Fi. (HORÁK, 2011)

- **SSID (Service Set ID)**: Již zmíněný údaj, který je názvem přístupového bodu (AP) a základním identifikátorem WiFi sítě. Je to 1 až 32místné jméno. Nastavuje se buďto manuálně na stanici nebo je tento údaj pravidelně automaticky vysílán. Potom se uživatel o SSID sám dotazuje. (HORÁK, 2011)
- **WEP** (**Wired Equivalent Privacy**)**:** Tato metoda byla volně integrována již v prvních generacích bezpečnostních protokolů, od protokolu 802.11b. Dnes se však moc nepoužívá, protože již není příliš bezpečná. Zjednodušený princip je takový, že odeslaná zpráva je zašifrována nějakým klíčem (40bitovým) a přijímač ji stejným klíčem dešifruje. WEP neověřuje samotného uživatele, ale pouze fyzickou adresu (MAC) jeho síťové karty. Heslo WEP zůstává nezměněno, dokud jej ručně nezměníme. (HORÁK, 2011) Tato metoda se zdála bezpečná, avšak brzy byla překonána a stala se nebezpečnou. Dokonce je volně ke stažení software, který dokáže WEP heslo rychle a jednoduše prolomit. (TANENBAUM, 2011)
- **802.1x:** Naštěstí si tento problém výrobci i uživatelé velmi rychle tento problém uvědomili. Vznikl tedy protokol EAP, který právě blokuje neoprávněným uživatelům přístup k síti. (HORÁK, 2011)
- **802.11i:** Jelikož byl později i tento způsob zabezpečení prolomen, byla zavedena nová robustná norma s názvem WiFi Protected Acces neboli WPA, které je nyní obměněno za WPA2, které je založeno na standardu AES (Advanced Encryption Standard) z roku 2002. (TANENBAUM, 2011) Protokol WPA je založen na průběžných automatických výměnách dynamicky vytvářených klíčů pro šifrovací procedury (řešení slabiny WEP). Dále se také zvětšila délka klíče pro šifrování – 256 bitů.

  Další zabezpečovací metodou je *filtrace MAC adres*, která se stará o povolování přístupů pouze vybraným uživatelům. Technologie je založena na

základě vypisování fyzických adres jednotlivých WiFi adaptérů. (HORÁK, 2011)

2.8 Způsoby zabezpečení sítí

2.8.1 Filtrace

„Filtraci rozumíme kontrolu procházejících paketů aktivním prvkem sítě na základě jeho obsahu a následné rozhodnutí, může-li být paket poslán dále, nebo ne. Filtr nemění obsah datových paketů.“ (DOSTÁLEK, 2008, str. 425) Filtraci si můžeme představit jako cenzuru, která může probíhat např. mezi poštovními zásilkami. Může probíhat na různých úrovních:

- Na linkové vrstvě – nastavuje se většinou na přepínačích (switch), ale mohou ji částečně provádět i firewally.
- Filtrace protokolů IP a TCP – ta se provádí na směrovačích (router), ale rovněž ji mohou provádět i firewally.
- Filtrace aplikačních protokolů – zde je možné, že dojde i ke změně přenášených paketů (při využití brány nebo proxy), a proto Dostálek tvrdí, že jde spíše o spekulaci, že se jedná ještě o filtraci. (DOSTÁLEK, 2008)

2.8.2 Firewall

Jedná se o jeden nebo více počítačů, které teoreticky „bezpečně“ oddělují vnitřní lokální síť mezi vnější sítí – Internetem tak, aby mohli uživatelé lokální sítě bezpečně přistupovat k informacím na Internetu. Firewall využívá více mechanismů, jako jsou proxy, brány, SOCKS nebo právě již zmiňovanou filtraci. Firewall je schopný, mimo to, že pracuje na vlastním PC, ukládat informace o provozu, tzv. logy, z kterých jsme schopni vyčíst dílčí akce, ale i vytvářet sumární přehledy – reporty. V dnešní době jsou aktivní firewally schopny automaticky vyčíst z logu potřebné informace a v důsledku toho způsobit jistou akci, otevřít nebo ukončit program apod. (DOSTÁLEK, 2008)

3 Analýza a popis současného stavu počítačové sítě

V následující části se již zaměříme na konkrétní problém, ke kterému se má bakalářská práce váže. Stručně si shrneme charakteristiku organizace, ve které budu počítačovou síť navrhovat, a přiblížíme si aktuální stav sítě v budovách.

3.1 Charakteristika organizace a její vývoj

Jedná se o mateřskou školu, s interním pojmenováním „mš1“, která se nachází na sídlišti v městské části Havířov - Šumbark. Areál tvoří tři dvoupodlažní, vzájemně propojené pavilony a zahrada, jejíž vzrostlá zeleň ji zčásti odděluje od okolní panelákové zástavby a zároveň poskytuje dětem příjemné a čisté prostředí k pobytu venku.

V současné době má mateřská škola 5 tříd a navštěvuje ji 125 dětí ve věku od 3 – 7 let.

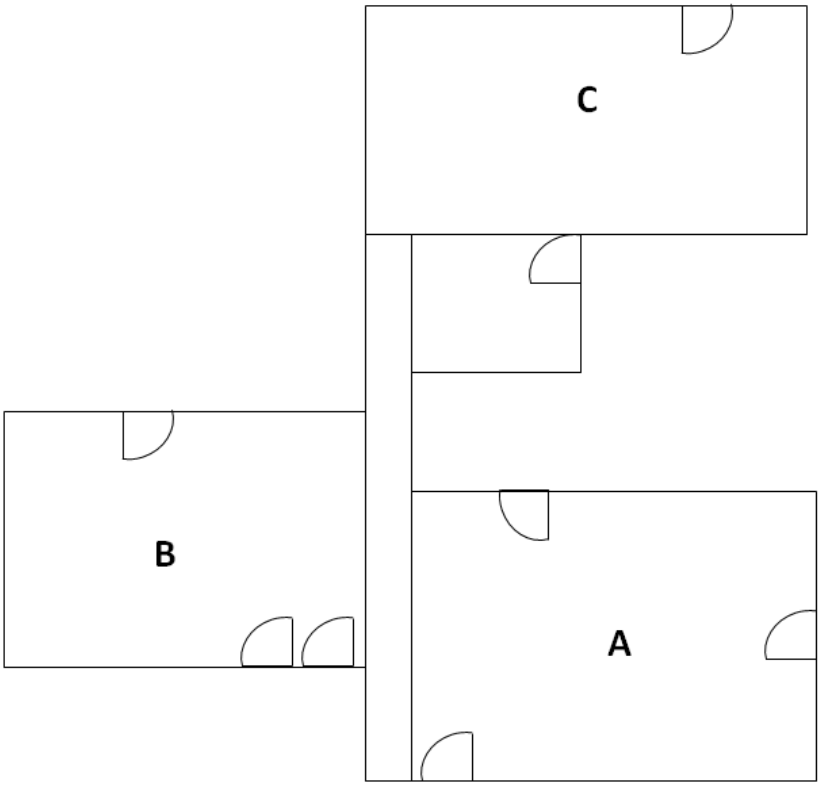
Součástí školy je školní jídelna. Obědy jsou však roznášeny do jednotlivých tříd.

K 1. lednu 2010 se mateřská škola rozšířila o 2 odloučená pracoviště:

- Mateřskou školu „mš2“ v Havířově - Městě se 2 třídami a kapacitou 44 dětí. Nyní je tato budova považována za hlavní, jelikož zde sídlí ředitel. Jídlo je dováženo.
- Mateřskou školu „mš3“ také v Havířově - Městě se 2 třídami a kapacitou 50 dětí. Škola má vlastní školní jídelnu.

3.2 Analýza budovy

Jak je z předchozích informací zřejmé, je mateřská škola rozdělena na kmenové pracoviště a dvě odloučená pracoviště. Já se budu zabývat pouze jedním z odloučených pracovišť, a to na ulici Petřvaldská. Na následujícím obrázku 3.1 vidíme nákres půdorysu budovy školky, ve které budu vytvářet počítačovou síť.



Obrázek 3.1: Půdorys mateřské školy „mš1“

Tuto budovu si pro lepší přehled rozdělíme na tři části, tedy na A, B a C. Jednotlivé části jsou spolu propojeny spojovací chodbou. V budově A se v přízemí nachází školní kuchyně, sklady, ředitelna a kancelář a v jejím horním podlaží je třída označená jako 3. oddělení. Budovy B a C jsou taktéž dvoupatrové, přičemž na každém patře je jedna třída. Celkem má školka tedy pět tříd, pět oddělení. Chodba je taktéž dvoupatrová.

Budova A

Zde se nachází ředitelna a kancelář ekonoma školy. V ředitelně, pro poznámku, však již sídlí vedoucí odloučeného pracoviště – zástupkyně školy, neboť ředitelka školy sídlí již ve změněné centrální budově, která se nachází na Sadové ulici (viz výše). Ředitelna je pro nás prioritní, protože se zde nachází zásuvka RJ-45 s přívodem Internetu do budovy. Síť je zde tvořena jedním Wi-Fi routerem značky LinkSys (splňuje normy 802.11 b/g), který vysílá bezdrátový signál pro dva přenosné počítače, které jsou právě v ředitelně. Využíván je však pouze jeden z nich. Tyto dvě místnosti jsou průchozí přes dveře. Hlavní router je také výchozí bránou do vnější sítě pro lokální počítače. Dále je veden síťový kabel (UTP) ze zmíněného

routeru do sborovny (využívána také jako klubovna například pro výrobu keramiky, tzn. příchozí i pro děti za dozoru pedagoga), kde je počítač, na kterém je také sdílený Internet a každý zaměstnanec zde má svůj přihlašovací účet.

V budově v přízemí se také nachází školní kuchyně, archiv, sklad a prádelna, ale tyto místnosti není potřeba se sítí nějak spojovat. Bližší nákres budovy nalezneme v příloze 1.

V horním patře budovy A se nachází třída – 3. oddělení, kde je počítač ve velice nevyhovujícím stavu bez jakéhokoliv připojení k síti. Součástí třídy je šatna, kumbál, místnost pro výdej obědů, umývárna a schodiště. Bližší nákres budovy nalezneme v příloze 1.

Budova B

V budově B, která je situována mezi budovami A a C, se nachází na každém patře třída, a to oddělení 1 v přízemí a oddělení 2 v patře. Součástí obou tříd je opět šatna, kumbál, místnost pro výdej obědů a schodiště. V obou třídách jsou dostačující stanice se systémy Windows XP, které bude možné připojit k síti. Rozmístění místností je v obou patrech totožné. Bližší nákres budovy nalezneme v příloze 1.

Budova C

Budova C se nachází nejdále od budovy A, na konci spojovací chodby, která je mj. také dvoupatrová. Zde jsou třídy – oddělení 4 (v 1. patře) a 5 (v přízemí). Opět stejné místnosti jako u předchozích tříd. Na 5. oddělení je starší počítač ještě se systémem Windows 2000, ale na 4. oddělení je nový počítač upravený pro děti, o kterém se zmíním později. Bližší nákres budovy nalezneme v příloze č. 1.

Tiskáren je po budovách rozmístěných celkem šest, přičemž pouze jedna z nich, která je zapojena při stolním počítači v ředitelně, má možnost síťového připojení. Není však pro síť nastavena a zatím to ani nebude potřeba. V ředitelně se nachází ještě jedna tiskárna/kopírka a vedle v kanceláři jsou dvě tiskárny (pouze jedna je barevná). Další tiskárna je ve sborovně a jedna je umístěna ve třídě na 4. oddělení spolu s novým počítačem.

3.3 Charakteristika správy sítě

Hlavní službou, která od 1. ledna 2010 běží na všech třech odloučených pracovištích této mateřské školy, je VPN – virtuální privátní síť, kterou vytvořila ostravská IT firma System Control s.r.o. Slouží pro připojení ke společným datům v centrále subjektu na Sadové z odloučených lokalit Místní a Petřvaldská. Připojením k centrále Sadová je možný přístup do sjednocené databáze matriky a společným datům ve sdílené složce.

Díky VPN jsou schopni pověření zaměstnanci a vedoucí pracovišť sdílet, otevírat, upravovat či mazat jednotlivé dokumenty na síťovém disku. Mezi tyto dokumenty patří především hlášení ke mzdám, pracovní smlouvy a informace o zaměstnancích, systém řádných dovolených a studijního volna, pracovní neschopnosti, přesčasové práce a odměny, informace o kroužcích, prázdné formuláře k vyplnění, informace o pronajímaných prostorách, informace o školném, pracovní a žákovské úrazy nebo například případné faktury za nakupovaný materiál.

Druhou službou v rámci VPN je velmi v ČR oblíbený systém Bakaláři, program pro vedení školní administrativy. Školka ji využívá zejména k evidenci dětí a inventarizaci majetku. Systém je otevřený. Uživatelé mohou například snadno reagovat na změny v blanketech vysvědčení, stovky připravených sestav lze modifikovat přímo v systému či standardními editory, zkušenější uživatelé mohou do systému doplňovat vlastní podprogramy. Díky otevřenosti a variabilitě vyhoví systém všem typům škol (ZŠ, ZUŠ, gymnázia, SOU, SŠ…). Používají jej také VOŠ a dokonce i několik VŠ (pro sestavení rozvrhu). Moderní prostředí programů využívá všech předností grafického operačního systému Windows - barevný tisk různými fonty, pohodlné jednotné ovládání apod. Data všech modulů jsou provázána, případnou změnu stačí provést na jednom místě. [4]

Koncové stanice

Všechny lokální počítače, které se nacházejí v budově školky, využívají operační systém Windows bez podpory funkcí serveru. Přenosné počítače se připojují k síti bezdrátově a stolní klasicky kabelem. V ředitelně se nachází celkově tři počítače, jeden stolní (procesor CPU s taktem 3.3 GHz, 4 GB RAM, 1 TB HDD atd.) a také dva výkonné notebooky (pouze jeden využívaný), které využívá pouze zástupkyně školy. Tyto počítače jsou velmi moderní, zhruba rok staré, s nainstalovaným operačním systémem Windows 7 (64bitové kopie). Vedle

v kanceláři jsou dva stolní počítače se staršími operačními systémy Windows XP, avšak s aktuálními aktualizacemi. Ve sborovně je stolní počítač s operačním systémem Windows XP s podobným sestavením jako v kanceláři. Pro odlehčení, platí zde tedy takové zlaté pravidlo, že ten nejvýše postavený zaměstnanec má nejlepší počítač. V tomto případě zástupkyně ředitelky, která opravdu s počítačem pracuje nejvíce. Všechny zmíněné počítače jsou bez podpory funkcí serveru, ale splňují bez problému základní požadavky pro práci se sítí i mimo ní.

Zbylé počítače v jednotlivých třídách mají starší systémy Windows XP nebo dokonce Windows 2000 a pracují většinou se zastaralým hardwarem. Sice by nejspíš zvládly základní práci v síti, ale v dnešní době jsou tyto stanice spíše nedostačující pro práci s moderními prvky na Internetu a o různých programech, například pro výuku malých dětí, nemluvě. Výjimku tvoří nový počítač na oddělení č. 4, kde jej školka obdržela z grantu města Havířov pro účely výuky dětí. Tento moderní počítač, jak můžeme vidět na obrázku 3.2, je nezvyklého tvaru, avšak uvnitř je umístěn výkonný stolní počítač IBM s operačním systémem Windows 7, tak, jak ho známe. Je v něm předinstalovaná sada zábavných aplikací pro děti. Počítač také není připojen k síti a nemá nainstalován žádný kancelářský ani antivirový program.

Obrázek 3.2: Moderní počítač uzpůsobený pro děti

V ředitelně je jedna multifunkční síťová (ethernetová) tiskárna, která však není pro síť využita. V kanceláři jsou dvě nesíťové tiskárny (jedna pouze černobílá) a fax. Další obyčejná tiskárna je ve sborovně a právě u nového počítače ze 4. oddělení.

Pro zmínku se v místnosti ředitelny nachází také telefonní ústředna, díky které je možné přepojování hovorů na telefonní linky v celé budově.

Internetové připojení

Školka má možnost připojení k Internetu déle než 10 let, momentálně přes provozovatele O2 Telefonica s připojením ADSL. Jedná se o nabídku Internet Optimal+ s rychlostí downloadu 20 Mbps a uploadu 2 Mbps, což dostatečně postačí pro práci typu čtení emailů apod. i pro ostatní počítače v budově.

Správa uživatelů

Nemalou výhodou je fakt, že každý uživatel, pedagog či jiný zaměstnanec, má již vytvořené své uživatelské jméno a heslo na lokálních stanicích a pověření pracovníci mají také své přihlašovací údaje k VPN. Mezi tyto uživatele patří ředitel a zástupce školy, vedoucí pedagog pracoviště na ulici Místní a ekonom školy, dva pedagogové k celkové inventarizaci majetku a jeden pedagog k inventarizaci knih. Přihlašování do systému VPN je jednotné. Po přihlášení do VPN jsou uživatelům dostupné síťové disky, které se nachází na vzdáleném serveru, umístěném na pracovišti u tvůrce této virtuální sítě v Ostravě-Třebovicích. Ani na lokálních stanicích ani v systému VPN nejsou přidělena uživatelům žádná zvláštní práva ke čtení či zápisu, všichni uživatelé mají plný přístup. Pouze na počítači, který je umístěn ve sborovně má každý uživatel (zaměstnanec) svůj účet (to dělá 16 účtů). Počítače v ředitelně a vedlejší kanceláři pracují ve standardní pracovní skupině „WORKGROUP“, ta však zde nemá zatím velký význam.

Zabezpečení

Většina prostorů v budovách je snímána pohybovými čidly po zapnutí alarmu v objektu, což jistě přispívá k její fyzické bezpečnosti proti vloupání a případnému odcizení majetku vč. výpočetní techniky.

Dalším zabezpečením je jednoduchá ochrana proti vnějším hrozbám v podobě firewallu zabudovaném na Wi-Fi routeru. Jiné ochrany (filtrace MAC adres, paketů apod.) nejsou na routeru aktivovány.

V neposlední řadě je na koncových stanicích v ředitelně, kanceláři a sborovně nainstalován antivirový program. Prohlížení obsahu na webu není žádným způsobem blokováno.

V budově byl před rozdělením školky na tři části jeden hlavní záložní zdroj UPS, který se však po té přesunul na centrální budovu. Nyní jsou tedy k třem stolním počítačům (v ředitelně a kanceláři) připojeny menší záložní zdroje pro případné výpadky elektřiny, které vydrží zhruba 20 minut se zapnutým počítačem. Je pravda, že převážně jsou pro organizaci směrodatné dokumenty, které jsou uloženy na serveru sdíleném sítí VPN, ale je jistě nepříjemné, když nám vypadne proud zrovna před uložením nově zpracovávaného dokumentu.

Zálohy dat nejsou z lokálních počítačů vytvářeny vůbec. Externí zálohy síťových disků pak provádí přímo správce sítě VPN, a to firma System Control. Na těchto discích se právě také nachází pro školku nejdůležitější dokumenty (již byly zmíněny v úvodu kapitoly).

Používaný software

Mateřská škola má na své počítače zakoupené hromadné licence pro kancelářské balíky Microsoft Office, avšak rozdílných verzí (2010 a 2007). Dále má zakoupeno hromadnou licenci pro antivirový program ESET NOD32 Antivirus verze 6, který je nainstalován na počítačích připojených k síti Internet. Výjimku tvoří PC ve sborovně, kde je antivir včetně personálního firewallu, ESET Smart Security 3 (také však vázáno na hromadnou licenci).

Na některých koncových stanicích na jednotlivých odděleních (třídách) jsou nainstalovány různé podpůrné aplikační programy a hry převážně pro děti předškolního věku. Ty se však na starých počítačích chovají velmi špatně.

Mezi další programy, které má školka zakoupeno patří Zoner Photo Studio 13, který je nainstalován pouze na stolním počítači v ředitelně. Slouží hlavně pro úpravu fotek z různých akcí, které se potom vystavují na nástěnkách, popř. zasílají rodičům dětí apod.

4 Návrh možného řešení k vytvoření počítačové sítě

V této kapitole se zaměřím na návrh řešení k vybudování počítačové sítě, která by měla splňovat pouze základní požadavky na sdílení souborů, tiskáren a Internetu. Řešení navrhnu dvě, a to v levnější a dražší variantě. Jelikož se v budovách vyskytuje pouze nepatrné množství síťových prvků, bude potřeba nakoupit většinu zařízení nových, případně i včetně koncových stanic. K veškerým návrhům co se týče rozložení síťových prvků a jejich nastavení jsem využil aplikačního síťového nástroje od firmy Cisco Packet Tracer verze 5.3.3. Základní práci v něm najdeme v příloze 2.

4.1 Výběr technologie, využití stávající sítě

Využití stávající sítě

Jak již bylo zmiňováno, v budově je přiveden Internet klasicky přes kabelové připojení do zásuvky RJ-45, která je umístěna v kanceláři školy. Ze zásuvky je vedena kroucená dvojlinka do Wi-Fi routeru značky LinkSys, který se chová také jako switch a rozvádí síť do ostatních počítačů. Notebooky jsou připojeny bezdrátově a tři stolní počítače (v ředitelně a dva v kanceláři) opět kabelem (síťový standard FastEthernet). Kabel vede také k další zásuvce do zdi, přes kterou vede až k poslednímu počítači napojenému k Internetu, a to do sborovny. Tímto je vyčerpán počet výstupů routeru s kabelovou přípojkou RJ-45.

Ve třídách jsou umístěny osobní počítače rozdílných vlastností, které byly školce bezplatně předány (repasovány), jakožto vytříděné, z Městského úřadu v Havířově. Všechny tyto stanice splňují sice požadavky pro připojení k síti, avšak jak již bylo zmíněno, nesplňují moderní požadavky pro práci s novými operačními systémy, případnými kancelářskými aplikacemi či výukovými programy pro malé děti. To je také jeden z důvodů, proč jsem navrhl dvě řešení pro vybudování nové sítě. Nákup koncových stanic je přeci jenom dražší záležitost, než nákup bezdrátových přístupových bodů.

Výběr technologií

Pro již zmíněné základní funkce sítě jsem ponechal síťový standard Fast Ethernet, odpovídající doporučení 802.3, aby byla síť schopna dosahovat dostačující přenosové rychlosti 100 Mb/s. Jedná se o budování sítě dle normy 100BASE-T, kdy je v prostorách rozprostřena kabeláž kroucených dvojlinek (UTP) kategorie 5e. Je zde nutno dodržet rozmezí kabeláže maximálně do 100 metrů, to však v našem případě není kvůli velikosti budovy problém.

Jako další důležitou technologií hraje v mé síti roli také bezdrátová síť Wi-Fi, která bude rozprostřena ve většině prostorů budovy pro rychlé připojení k síti a také pro případný narůstající počet připojených zařízení k síti. Dostupné jsou standardy 802.11 b/g/n, které pracují v pásmech 2,4 GHz a 5 GHz. Volbu však nechám zvolenou na automatických režimech samotných přístupových bodů, protože pro nás nejsou rozdílné vlastnosti těchto standardů až tak směrodatné. Pásmo 5 GHz je pak i tak u nás zakázáno, automaticky se volí pásmo 2.4 Ghz.

Fyzická topologie sítě je stromová, která se v tomto případě odvíjí od hvězdicové. Hlavní využívané prvky sítě jsou switche a přístupové body (AP) Wi-Fi, ke kterým je možnost se kdykoliv ihned připojit. Tyto prvky jsou spojeny mezi zařízeními buďto již zmíněnou kabeláží nebo bezdrátovým médiem.

Řešením jsou dva návrhy, které se od sebe liší právě především rozsahem využití jednotlivých síťových technologií a tím se odvíjející celkovou cenou pořízení.

4.1.1 Firma pro výstavbu fyzické struktury

Pro výstavbu fyzické struktury sítě mezi jednotlivými budovami a místnostmi jsem si vybral firmu FLAME System s.r.o se sídlem v Ostravě. Firmu jsem zvolil především kvůli bohatému spektru referencí, mezi něž patří také Vysoká škola báňská – TU Ostrava nebo Ostravská Univerzita v Ostravě. Dále však také pro krátkou vzdálenost mezi firmou a školkou, její dostupností a z toho plynoucím nízkým dopravním nákladům.

Více informací o této firmě naleznete na oficiálních stránkách firmy na internetové adrese www.flame.cz.

4.2 Návrh cenově levnější varianty

V první navrhované variantě budu brát v úvahu především finanční náklady spojené s nákupem nových zařízení a síťových prvků a budu se snažit o minimalizaci celkových nákladů. Hlavní využitou technologií bude bezdrátový přenos. Samozřejmostí bude tedy taky svobodný pohyb s přenosnými zařízeními kdekoliv po budově s automatickým připojením k nejsilnějšímu přístupovému bodu. Tato varianta nebere v úvahu nákup nových koncových zařízení pro jednotlivá oddělení, tudíž bude práce na stávajících počítačích stále omezená a nevyzpytatelná.

Hlavním cílem této varianty bude tedy:

- Propojení všech počítačů bezdrátově, a to umístěním různě po budovách několika bezdrátových přístupových bodů. Beru v úvahu také vybavení stolních počítačům externími Wi-Fi adaptéry, aby byly schopné provozu v bezdrátových sítích standardu 802.11. Způsob připojení k síti u již připojených PC zůstane zachován.
- Nastavení pracovní skupiny počítačů, ve které budou moci uživatelé sítě využívat sdílení souborů a tiskáren a na ně aplikovat také určitou ochranu zabezpečení. Vytvořit přihlašovací systém uživatelských jmen a hesel na koncových stanicích.
- Nakoupení alespoň základního balíku kancelářských aplikací pro koncové stanice, na kterých bude poté možné spouštění a případná úprava sdílených pracovních dokumentů.
- Nakoupení a nainstalování softwaru pro zabezpečení koncových stanic proti virům a jiným hrozbám hrozícím při prohlížení stránek Internetu, čtení elektronické pošty apod.
- Zajištění adekvátní firmy, která bude schopna fyzicky propojit sítě mezi zdmi v jednotlivých budovách (pořízení zásuvek a potřebné kabeláže nechávám na firmě).
- Zásuvky RJ-45 budou vždy po jednom kusu v každé budově pro připojení bezdrátového přístupového bodu. Umístění nechávám na firmě, která má tuto realizaci na starosti, abych jim svým umístěním zásuvek nepřitížil práci a tím např. nezvýšil výslednou cenu za realizaci.

4.2.1 Doporučený hardware

V síti se již nachází jeden hlavní bezdrátový router, který má čtyři fyzické výstupní porty pro zapojení LAN sítě. Proto musíme do sítě přidat další zařízení, které nám možnost více koncových stanic rozvětví. K vytvoření první navrhované varianty bude tedy zapotřebí zakoupit dva switche. První bude pro dva počítače umístěné v kanceláři, druhý bude sloužit k připojení přístupových bodů k bezdrátové síti. Umístěn bude v ředitelně a povedou z něj kabely do zásuvek ve zdi, které budou provedeny, až do jednotlivých budov. Typ switche (zmíněný v tabulce 4.1) jsem vybral z důvodu, že má možnost až 8 výstupních portů (pozdější přidání dalšího počítače) a také kvůli značce, se kterou mám dobré zkušenosti. Dále je potřeba zakoupit dva přístupové body (access point), přičemž jeden bude umístěn na budově B (oddělení 1 a 2) a druhý na budově C (oddělení 4 a 5). Počítač na oddělení 3 se nachází ve stejné budově, odkud vysílá i hlavní Wi-Fi router. Tento počítač se tedy může napojit bezdrátově přímo na něj. Přístupové body sice nepodporují normu 802.11n, ale ta je pro naše účely téměř nepotřebná. Antény přístupových bodů musí být nasměrovány tak, aby měli dosah mezi oběma patry v každé budově. V neposlední řadě musíme opatřit všechny stolní počítače v jednotlivých odděleních externími Wi-Fi adaptéry pro příjem bezdrátového signálu Wi-Fi. Nejlepší způsob se mi zdá přes konektor USB. Vybraný typ jsem zvolil především kvůli jeho velikosti a tím zamezení případným zavadění například nohou, jelikož počítače stojí na podlaze.

Kabeláž, zásuvky a zbylé potřebné komponenty spadají do režie firmy, která si tyto položky přičte k celkové ceně za realizaci. Proto tyto komponenty v návrhu neuvádím.

Tabulka 4.1: Seznam doporučených komponent u levnější varianty

Název komponenty	Popis	Počet ks	Cena vč. DPH / ks
TP-LINK TL-SF1008D	switch, 8 portů, 10/100Mbps, RJ45, desktop, IEEE802.3, 802.3u, 802.3x, TCP/IP, auto MDI/MDIX	2	232,-
TP-LINK TL-WA500G	bezdrátový přístupový bod, 802.11b/g, 54Mb/s, 1x LAN, 1xRSMA, AP, Bridge, Klient, Repeater, WDS, 64/128-bit WEP, WPA/WPA2 PSK TKIP/AES, firewall, NAT, eXtended Range, čip Atheros	2	549,-

Tenda W311MI	Wi-Fi síťový USB adaptér, USB, 150Mbps, 802.11b/g/n Draft 2.0, WEP, WPA, WPA2, Ad-Hoc, SoftAP, QoS, WMM, čip Realtek RT3370	5	219,-

Navržený hardware je vybrán a popisky převzaty z nabídky internetového obchodu Alfa Computer a.s (dále jen alfacomp.cz) [5].

V příloze č. 3 vidíme fyzické uspořádání jednotlivých zařízení a jejich zapojení.

4.2.2 Výběr vhodného softwaru

Jelikož tato varianta nebere v úvahu nákup nových počítačů, je výběr vhodného softwaru pro potřebné účely téměř zbytečné. Stávající počítače by nebyly schopny efektivně kancelářské aplikace využívat, protože většinou nesplňují ani minimální hardwarové požadavky těchto programů. Antivirový program by byl potom realizovaný s freeware licencí, které však většinou nesplňují úplnou ochranu před hrozbami na Internetu i v síti. Takovými programy jsou například Avast Free Antivirus nebo Microsoft Security Essentials.

4.3 Návrh cenově dražší varianty

Druhou variantu jsem navrhl pro případ, že by byla školka schopna investovat větší peněžní částku pro svou síť. Hlavní změna oproti první variantě je, že navrhuji na každou třídu (kromě 4. oddělení) nový stolní počítač a že tyto PC na jednotlivých třídách budou zapojeny do sítě kabelově přes zásuvku. Zásuvky budou umístěny přímo ve třídách tak, aby nemusel být kabel moc dlouhý. Jejich konkrétní umístění opět nechávám na firmě, musí však splňovat podmínku, aby byla zásuvka blízko koncové stanice. Výhoda spočívá určitě v tom, že se tímto spojením snižuje riziko vniknutí do sítě cizí osobou a také například kvalitou rychlosti připojení k Internetu. Odpadají také různá rádiová rušení signálu apod.

Hlavní cíle této varianty zůstávají totožné jako u předchozí varianty. Liší se pouze v technologii připojení koncových stanic ve třídách k síti.

4.3.1 Doporučený hardware

U tohoto návrhu jsem tedy nenavrhl zakoupení bezdrátových bodů, avšak stále platí potřeba dvou switchů. Jeden bude umístěn v kanceláři pro dva stolní počítače a druhý opět v ředitelně odkud povedou kabely do zásuvek umístěných ve zdi. Ty pak povedou přes zdi až do jednotlivých tříd k druhým koncům a budou zakončené zásuvkou. U koncových stanic odpadá nutnost nakupování dalšího hardwaru pro připojení k síti, vystačíme si klasickou síťovou kartou, která je v nových počítačích již součástí.

Počítače jsem tedy navrhl již sestavené již s USB klávesnicí a optickou myší od výrobce Lenovo. Konkrétně typ Lenovo H430 stolní počítač nabízí celou řadu funkcí pro zábavu, a to všechno za velmi rozumnou cenu. Díky vysokému výkonu 2. nebo 3. generace procesorů Intel je ideálním společníkem pro každé oddělení. Poslouží dobře pro prohlížení webových stránek, editaci dokumentů, přehrávaní videa anebo editaci školních fotografií.

Srdcem této sestavy je dvoujádrový procesor Intel 2. generace procesorů Sandy Bridge, který pracuje na frekvenci 2.9 GHz. Sekundují mu 4 GB pamětí DDR3 a rychlý 500 GB pevný disk. O konektivitu se postará VGA či HDMI port, které jsou doplněny šesticí USB portů 2.0. Grafický výkon obstarává výkonná grafická karta nVidia GT620 s 1 GB vlastní paměti.

Díky technologie Lenovo Enhaced Experience 3 jsou starty systému Windows až o 40 % rychlejší než u konkurence se stejnými komponenty. [5]

Monitory jsem zvolil od předního světového výrobce Hawlett-Packard, konkrétně typ HP 2011x. Monitor HP 2011x nabízí dokonalou kombinaci obrazového výkonu, elegantního designu, ekologických funkcí a LCD panelu podsvíceného diodami LED s úhlopříčkou 50,8 cm (20"), který vám pomůže zlepšit uživatelské pohodlí. Stylové ultratenké monitory HP 2011x se v kancelářském prostředí skvěle vyjímají, aniž by zabíraly cenné místo a přizpůsobitelné naklonění umožňuje jasné zobrazení z mnoha úhlů a zajišťuje tak větší pohodlí a produktivitu. Ostrý a čistý obraz na obrazovce s nativním rozlišením 1 600 x 900, dynamickým kontrastem 3 000 000:1, pozorovacím úhlem až 170° a rychlou odezvou 5 ms. Široké možnosti připojení zajišťují vstupy rozhraní DVI-D a VGA. Monitor HP 2011x díky použití diod LED bez obsahu rtuti, díky sklu displeje bez obsahu arzenu, certifikaci ENERGY STAR a registraci EPEAT Silver pomáhá snížit dopad na životní prostředí. [5]

V následující tabulce 4.2 je uveden rozpis navržených zařízení. Kabeláž, zásuvky a zbylé potřebné komponenty opět spadají do režie firmy, která si tyto položky přičte k celkové ceně za realizaci.

Tabulka 4.2: Seznam doporučených komponent u dražší varianty

Název komponenty	Popis	Počet ks	Cena vč. DPH / ks
TP-LINK TL-SF1008D	switch, 8 portů, 10/100Mbps, RJ45, desktop, IEEE802.3, 802.3u, 802.3x, TCP/IP, auto MDI/MDIX	2	232,-
TP-LINK TL-WA500G	bezdrátový přístupový bod, 802.11b/g, 54Mb/s, 1x LAN, 1xRSMA, AP, Bridge, Klient, Repeater, WDS, 64/128-bit WEP, WPA/WPA2 PSK TKIP/AES, firewall, NAT, eXtended Range, čip Atheros	2	549,-
Lenovo IdeaCentre H430	sestava PC, Intel Pentium G645 2.9GHz DC, 500GB (7200), 4GB DDR3, čtečka, DVDRW, VGA NV GT 620 1GB, Intel H61, glan, 6x USB, VGA, HDMI, USB klávesnice a optická myš, Windows 8	4	9 999,-
HP 2011x 20" černý	monitor LCD, širokoúhlý 16:9, TFT TN, LED podsvícení, 1600x900, 3mil:1, 250cd, 5ms, D-Sub, DVI-D	4	2 590,-

Navržený hardware je vybrán a popisky převzaty také z nabídky internetového obchodu Alfa Computer a.s (dále jen alfacomp.cz). [5]

V příloze č. 3 můžeme vidět fyzické uspořádání jednotlivých zařízení a jejich zapojení u dražší varianty.

4.3.2 Výběr vhodného softwaru

Jak již bylo zmíněno, na koncových stanicích v jednotlivých odděleních by měly být nainstalovány některé kancelářské nástroje pro otevření potřebných dokumentů. Zvolil jsem moderní balíček Microsoft Office 365 Small Business Premium CZ s předplatným na jeden rok a možností nainstalování současně na pět stanic. V balíku nechybí Word, Excel,

PowerPoint nebo např. Outlook a antivirový program. Cena tohoto softwaru je 3.799,- Kč vč. DPH v internetovém obchodě Alza.cz. Jelikož jsou již na jiných počítačích nainstalovány antiviry od výrobce ESET, byl rovněž zvolen. Vybral jsem balíček ESET Endpoint Security za 6.225,- Kč vč. DPH s platností na 1 rok, pro pět koncových zařízení vč. nového počítače na 4. oddělení. Cenová nabídka je převzata s oficiálních stránek společnosti ESET http://koupit.eset.cz.

4.4 Nastavení zařízení

Tato kapitola je zaměřena na nastavení a možnosti jednotlivých prvků. Převážně jejich základní nastavení pro chod ve školní síti a také zabezpečení bezdrátové sítě.

4.4.1 Nastavení IP adres koncových zařízení

V síti již máme několik počítačů, některé využité ze stávajícího stavu a v jednotlivých třídách, které byly nově připojeny k síti. Jelikož se jedná o velmi malou síť s malým počtem koncových zařízení, je zde již z minulosti nastaven rozsah adres pro třídu C, která má tvar 192.168.xxx.xxx, a její příslušnou masku sítě 255.255.255.0. Adresy jsou ke všem počítačům přirazeny automaticky pomocí DHCP serveru implementovaného přímo na hlavním Wi-Fi routeru v ředitelně. Třída je standardně určena pro 253 koncových stanic, ale router je již nastaven pouze pro 50 zařízení. Toto nastavení zůstane pro stávající počítače zachováno v obou variantách návrhů s tím rozdílem, že pro nové počítače v síti (to je 5 ks), vyhradíme určité adresy, které budou k jednotlivým počítačům přiřazovány vždy stejně. To znamená, že ke každé MAC adrese bude přiřazena jedna IP adresa. Celkem je v síti tedy 5 počítačů, které mají dynamicky přidělenou adresu pomocí služby DHCP a 5 počítačů s pevně stanovenou adresou. V nastavení pro 50 zařízení zůstává stále dostatečný prostor pro případné připojení dalších bezdrátových zařízení např. přenosných počítačů nebo i smartphonů.

Níže uvedená tabulka 4.3 zobrazuje nastavení námi vyhrazených IP adres.

Tabulka 4.3: Seznam vyhrazených IP adres pro stanice ve třídách

Zařízení	IP adresa
Wi-Fi router	192.168.0.1
PC na odd. 1	192.168.0.21
PC na odd. 2	192.168.0.22
PC na odd. 3	192.168.0.23
PC na odd. 4	192.168.0.24
PC na odd. 5	192.168.0.25

4.4.2 Nastavení bezdrátových zařízení

Hlavní Wi-Fi router je připojen k Internetu staticky. Nastavení je v tomto případě poskytnuto smluvně poskytovatelem Internetu a při změně by jej nebylo možné se k Internetu připojit. Nastavení SSID, zabezpečení a autentifikace bezdrátové sítě ponecháme také ve stávajícím stavu, který využívá zabezpečení prostřednictvím WPA2 a šifrování hesel AES. Wi-Fi pracuje pouze se sítěmi v režimu 802.11 b/g, necháme tedy volbu výběru nastavenou se standardním rádiovým rozsahem 20 MHz. Jméno sítě (SSID) zůstává i nadále odkryto a broadcastově vysíláno. Filtraci MAC adres necháváme nevyužitou, může být však v budoucnu využita. Router má aktivovaný již implementovaný firewall pro lepší bezpečnost přístupů z vnějšku. Administrátorské přihlášení k nastavení routeru zůstává zachováno.

Jediným bodem, který nás momentálně zajímá, je doplnit nastavení služby DHCP o vyhrazené rezervace pro jednotlivé počítače ve třídách. To znamená, jak již bylo zmíněno, k jednotlivým MAC adresám přiřadit IP adresy, které budou na počítačích ve třídách vždy stejné.

Jelikož má router staticky přidělenou adresu 192.168.0.1, je na DHCP server nastaveno adresování od adresy 192.168.0.2 po 192.168.0.51, tedy pro 50 počítačů.

Pro ostatní dva přístupové body je potřeba nastavit stejné parametry jako u Wi-Fi routeru, aby nebylo potřeba při přechodu do jiných místností volit jiné nastavení sítě v přenosných zařízeních. To znamená stejné SSID, stejné heslo a stejný vysílací kanál, na kterém se signál šíří tak, aby bylo vytvořeno překrývání a tím bezproblémové přecházení mezi vysílacími body. Pokud bychom tyto parametry pozměnili, musely by být vysílací

kanály v rozestupu alespoň 3 kanálů, aby se tyto kanály navzájem nerušily. Vysílacích kanálů je u režimu 802.11 b/g třináct.

4.4.3 Nastavení pro sdílení souborů a tiskáren

Základní podmínkou pro práci se sdílenými soubory v naší síti je, aby měl každý počítač své pojmenování, konkrétně *Úplný název počítače*, a aby byly koncové stanice zařazeny do stejné pracovní skupiny. Počítače jsem pojmenoval stejně, jako je na grafických návrzích rozmístění sítě na obrázcích umístěných v příloze 3, a budou umístěny do pracovní skupiny se standardním názvem *WORKGROUP*. V síti může být i více pracovních skupin, pro naše účely nám však prozatím postačí jen jedna.

Dále je potřeba vytvořit sdílenou složku, ke které budou mít ostatní počítače přístup. Jelikož je počítač v ředitelně nejrychlejší, disponuje dostatečným úložným prostorem a je spuštěn téměř celou pracovní dobu, umístíme sdílenou složku na disk v tomto počítači. Sdílené dokumenty pak převážně vytváří právě zástupkyně ředitele, která s tímto počítačem pracuje. Ta musí mít o sdílených souborech úplný přehled. Většinou se bude jednat o stručná i obsáhlá oznámení ze strany vedení, ale i o formuláře k vyplnění pro pedagogy, tj. kolik dětí v den přišlo a jiné zprávy. Dále například o fotografie či videa pořízené při školních akcích. Na koncových stanicích se potom musí tato síťová složka mapovat a umístit třeba na pracovní plochu pro rychlý přístup. Složky budou nastaveny pro sdílení s částečným přístupem, tedy pro vytváření, čtení a přepisování. Mazání souborů a podsložek bude zpřístupněno pouze pro administrátora sdílené složky, v našem případě zástupkyně školy. Pro přístup ke sdílené složce bude potřeba zadat vlastní uživatelské heslo. Složka bude tedy chráněna heslem.

Možnosti tisku v síti zatím není potřeba, jelikož mají pedagogové volný přístup k počítačům s tiskárnou v kanceláři nebo ve sborovně. Jediná síťová tiskárna je umístěna v ředitelně a ta není volně přístupná, tudíž je nevyužita. Pokud by však měly být síťové tiskárny do budoucna realizovány např. na každé budově, je tato možnost uvedení do provozu jednoduchá, a to označením tiskárny za sdílenou v síti. Pravděpodobně by však bylo lepší umístit na každou třídu vlastní tiskárnu (4. oddělení již má).

4.5 Finanční analýza obou variant

V následující kapitole si v několika tabulkách (4.4, 4.5, 4.6, 4.7 a 4.8) shrneme a porovnáme finanční náklady obou mnou navrhovaných variant. Vybral jsem konkrétní hardwarové komponenty s přesnými částkami za zboží. Ceny jsou uvedeny včetně DPH. Celkové náklady na realizaci se mohou lišit v závislosti nákladů, které bude požadovat firma za odvedenou práci. Proto je tato finanční analýza pouze orientační.

Firma si účtuje za provedení projektových a přípravných prací, dále za expertní práce typu vedení kabeláže zdmi, montáž zásuvek atd. V neposlední řadě si účtuje dopravu ze svého stanoviska v Ostravě do Havířova za každý den. Plánovaná doba instalací je zhruba čtyři pracovní dny po 6 hodinách denně.

Tabulka 4.4: Finanční analýza HW komponent levnější varianty

Komponenta	Typ	Počet ks	Cena za ks	Cena
switch	TP-LINK TL-SF1008D	2	232,-	464,-
přístupový bod	TP-LINK TL-WA500G	2	549,-	1 098,-
WiFi adaptér	Tenda W311MI	5	219,-	1 095,-
Celková cena				**2 657,-**

Tabulka 4.5: Finanční analýza HW a SW draží varianty

Komponenta	Typ	Počet ks	Cena za ks	Cena
switch	TP-LINK TL-SF1008D	2	232,-	464,-
přístupový bod	TP-LINK TL-WA500G	2	549,-	1 098,-
PC sestava + OS	Lenovo IdeaCentre H430 s Windows 8	4	9 999,-	39 996,-
LCD monitor	HP 2011x 20"	4	2 590,-	10 360,-
kancelářský balík	Microsoft Office 365 Small Business Premium	1	3 799,-	3 799,-
antivirová ochrana	ESET Endpoint Security	1	6 225,-	6 225,-
Celková cena				**61 942,-**

Ceny jsou uvedeny s DPH. Převzato z internetových obchodů www.alfacomp.cz, www.alza.cz a www.eset.cz.

Tabulka 4.6: Finanční analýza fyzické realizace levnější varianty

Popis práce	Orientační doba (hod.)	Cena za 1 hod.	Cena
projektové/přípravné práce	4	500,-	2 000,-
expertní práce u zákazníka	20	900,-	18 000,-
materiál (kabeláž, zásuvky atp.)			1 000,-
doprava (tam i zpět)	150 km	12 Kč/km	1 800,-
Celková cena bez DPH			**22 800,-**
Celková cena s DPH (20 %)			**27 360,-**

Tabulka 4.7: Finanční analýza fyzické realizace dražší varianty

Popis práce	Orientační doba (hod.)	Cena za 1 hod.	Cena
projektové/přípravné práce	4	500,-	2 000,-
expertní práce u zákazníka	24	900,-	21 600,-
materiál (kabeláž, zásuvky atp.)			1 500,-
doprava (tam i zpět)	150 km	12 Kč/km	1 800,-
Celková cena			**26 900,-**
Celková cena s DPH (20 %)			**32 280,-**

Jednotlivé ceny jsou uvedeny bez DPH, převzato z www.flame.cz.

Tabulka 4.8: Celkové náklady pro jednotlivé varianty návrhů

Položky	Levnější varianta	Dražší varianta
HW a SW	2 657,-	61 942,-
Fyzická realizace sítě	27 360,-	32 280,-
Celkové náklady	**30 017,-**	**94 222,-**

5 Zhodnocení navrženého řešení a následná implementace

Zhodnocení z finančního hlediska

Z předchozí kapitoly je jasně viditelný rozdíl nákladů obou navrhovaných variant. Levnější varianta byla vykalkulována na částku 30 017 Kč a dražší o 64 205 Kč více, tedy 94 222 Kč. Znatelný rozdíl v celkových sumách je zapříčiněn hlavně nákupem nových koncových stanic včetně příslušenství pro jednotlivá oddělení a potřebným programům pro základní práci s nimi. Jedná se o nákup kancelářského balíku Microsoft Office 365 a ESET Endpoint Security s roční licencí pro pět počítačů. Co se týče nákupu hardwaru a softwaru, činí nákup počítačů a programů okolo 97,5 % při dražší variantě, konkrétně pak 60 380 Kč. U levnější varianty jsem kancelářský balík a antivirový program záměrně nenavrhl z důvodu vysokých minimálních požadavků na počítač. Jak již bylo zmíněno, počítače jsou kromě nového počítače na 4. oddělení ve velmi kritickém stavu, tzn. pro dnešní moderní programy a práci na Internetu téměř na odpis. Pokud by vedení požadovalo tento software zakoupit u levnější varianty alespoň na nový počítač na 4. oddělení, navrhl bych koupi u stejných prodejců pouze však s licencí pro jednu stanici. Antivirová ochrana pro ostatní počítače by potom byla realizována pomocí nějakého freeware antivirového programu. Fyzická realizace sítě firmou se pohybuje u obou variant okolo 30 tisíc Kč. Rozdíl částek u navrhovaných variant činí 4 920 Kč, což zapříčiňuje u dražší varianty delší pracovní dobu firmy z důvodu protažení kabeláže až do jednotlivých tříd a samozřejmě o něco více potřebného materiálu.

Zhodnocení navrhovaných variant

Myslím si, že je pro mateřskou školu výhodná investice do první i do druhé navrhované varianty. První varianta je sice levnější, ale nepočítá s nákupem nových koncových zařízení, a proto nebude práce se starými počítači i nadále zcela uživatelsky přátelská a bude nepřijatelná jako doposud. Sice bude možné se připojit k Internetu a sdílet soubory, ale práce bude značně omezená. Na druhou stranu budou v budovách rozmístěny bezdrátové body k jednoduchému přístupu k síti z jiných přenosných zařízení, jako je notebook nebo smartphone. To je výhodné v případě, že by pedagogové vlastnili tyto zařízení sami. K síti se pak připojí pomocí přihlašovacího hesla sítě. Síť je pro tuto možnost dostatečně připravena díky dynamickému přidělování IP adres službou DHCP.

Druhá varianta návrhu je naopak znatelně dražší, avšak zahrnuje koupi nových koncových stanic (stolních počítačů) pro jednotlivá oddělení. Učitelé mohou tyto počítače využít jak pro svou práci s dokumenty, popř. Internetem, ale také jako učební nástroj a pomůcku pro děti formou různých aplikací dětem určeným či výukových videí. Tato varianta pak nenabízí možnost připojení se k síti bezdrátovým způsobem přes jiné zařízení. Síť je však v tomto případě obecně lépe zabezpečena proti cizímu vniknutí, některým z přístupových bodů, protože jsou nové počítače propojeny kabeláží.

5.1 Implementace sítě

Jelikož je pro takto rozsáhlou rekonstrukci v prostorách školky na ulici Petřvaldská zodpovědnou osobou zástupkyně školy, rozhodla se tak pro uskutečnění druhé navrhované varianty, a to hlavně z důvodu koupi nových počítačů pro jednotlivá oddělení a s nimi spojenou jednodušší práci pro pedagogy a novou možnosti vyučování.

Realizaci návrhu však bohužel nechce uskutečnit v termínu odevzdání této bakalářské práce z důvodu jejího odkladu. Realizace je postupně odložena na období letních prázdnin, kdy nebudou v mateřské škole děti. Tyto práce by dle zákona č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), neměly být realizovány v přítomnosti dětí, aby tak byla zachována jak jejich bezpečnost, ale také bezpečnost zaměstnanců organizace. Realizace by se měly uskutečnit po částech, kdy se o letních prázdninách bude instalovat kabeláž a postupně budou z finančního hlediska dokupovat jednotlivé počítače.

6 Závěr

Cílem této práce bylo navrhnout a implementovat síť pro mateřskou školu. Po zanalyzování aktuálního stavu jsem zjistil, že ve školce je již určitá technologie spjatá s problematikou sítí již použita. Jednalo se zejména o připojení k Internetu a k VPN pro vedoucí pracovníky. První cíl byl tedy splněn.

Druhým cílem bylo na základě provedeného zjištění navrhnout možná řešení k vytvoření kompletní sítě LAN vč. výběru případně nového síťového HW a SW s co nejnižšími pořizovacími náklady. Vytvořil jsem proto dvě varianty návrhů, přičemž první byla s nižšími náklady a druhá s vyššími v závislosti převážně na nákupu nových koncových zařízení vč. potřebného příslušenství do jednotlivých tříd a na využité technologii připojení. Dále jsem také vybral velmi prosperující firmu, která je schopna vytvořit velice kvalitní fyzickou infrastrukturu sítě mezi jednotlivými budovami za přijatelnou cenu.

Adresování v síti jsem ponechal stávajícím nastavením sítě pomocí služby DHCP, přičemž jsem rezervoval adresy pro nové počítače v síti umístěné v jednotlivých odděleních. Návrhy, jak je vidět na výše umístěných obrázcích, včetně nastavení adres jsem zpracoval v programu CISCO Packet Tracer a nastavil přes něj síť pro sdílení Internetu a případné sdílení souborů a tiskáren a tím jsem splnil další třetí dílčí část cíle.

Co se týče zabezpečení sítě, funguje zde přihlašování ke koncovým stanicím pomocí uživatelského jména a hesla. Na všechny koncové stanice připojené k Internetu je aplikován antivirový program s ochranou personálního firewallu. U bezdrátových sítí potom funguje přihlašování k síti pomocí silného zabezpečení s šifrováním hesla a vestavěný firewall u spojujícího zařízení s vnějškem prostřednictvím Wi-Fi routeru. Ostatní zabezpečení jsem pro nesouhlas zástupkyně ředitelky školy nenavrhl, mám na mysli skrytí bezdrátové sítě a filtrování MAC adres, protože by měla být síť viditelná a přístupná i z jiných přenosných zařízení jako je notebook nebo smartphone, samozřejmě až po zadání správného přístupového hesla k síti.

Tím se dostávám k poslednímu cíli práce, a to finanční analýze, zhodnocení a předání návrhu. Jak je zřejmé z uvedených tabulek, varianty se od sebe liší zhruba o 64 tisíc Kč. Takto převratný rozdíl je zapříčiněn zejména nákupem nových koncových zařízení a využití jiné technologie připojení. Kompetentní pracovník k nákupům takových rozsáhlých realizací, zástupkyně ředitelky školy, byla obeznámena s jednotlivými návrhy. Rozhodnutí padlo na

druhou navrhovanou variantu, a to hlavně z důvodu koupě nových počítačů do jednotlivých tříd. Rozhodla však prozatím o odložení realizace tohoto návrhu o několik měsíců. Konkrétně je realizace odložena na období letních prázdnin, kdy nebudou v mateřské škole děti, aby byla zajištěna maximální bezpečnost při práci a nemalé rekonstrukci. Tato bakalářská práce by měla převážně sloužit pro MŠ i jako strategický plán, podle kterého bude realizace probíhat.

V úplném závěru musím říct, že i přes nedokončení plánované implementace byla pro mě práce velkým přínosem, protože je především praktická. Rád bych měl znalost vytváření sítí do budoucna stále uchovanou pro případné zaměstnavatele, či k případnému vytvoření nějakého mnou založeného obchodního subjektu, který by se mohl touto rozsáhlou problematikou zabývat.

Seznam použité literatury

a) Odborná literatura

[1] TANENBAUM, Andrew S. a David J. WETHERALL. Computer Networks (5th Edition). 5th ed. Boston: Prentice Hall, 2010. ISBN 978-0132126953.

[2] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

[3] DOSTÁLEK, Libor a Alena KABELOVÁ. Velký průvodce protokoly TCP/IP a systémem DNS. 5. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.DE PELSMACKER, Patrick, Maggie GEUENS a Joeri VAN DEN BERGH. *Marketingová komunikace*. Překl. Vlasta Šafaříková. 1. vyd. Praha: Grada Publishing, 2003. 581 s. ISBN 80-247-0254-1.

b) Internetové zdroje

[4] SYSTEMCONTROL S.R.O. Bakaláři [online]. ©2012 [cit. 2013-04-13]. Dostupné z: http://www.systemcontrol.cz/index.php?option=com_content&view=article&id=28&Itemid=91

[5] ALFA COMPUTER A.S. [online]. ©2004-2013 [cit. 2013-04-24]. Dostupné z: http://www.alfacomp.cz

c) Jiné zdroje informací

[6] Studijní materiály pedagoga VŠB-TU Ing. Petra Rozehnala Ph.D.

[7] BABIUCH, Marek. Studijní materiály: Konfigurace síťových prvků a protokolů. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2011. ISBN 978-80-248-2764-3.

Seznam tabulek

Seznam obrázků

Seznam zkratek

%	procento
AP	Access Point
apod.	a podobně
atd.	a tak dále
BOOTP	Bootstrap Protocol
GHz	Gigaherz
HDMI	High-Definition Multimedia Interface
hod.	hodina
HP	Hawlett-Packard
IEEE	Institute of Electrical and Electronics Engineers
Kč	Koruna česká
MAC	Media Access Control
Mbps	Megabit per second
např.	například
obr.	obrázek
popř.	popřípadě
RARP	Reverse Address Resolution Protocol
SOCKS	SOCKet Secure
SSID	Service Set Identifier
tab.	tabulka
TCP/IP	Transmission Control Protocol / Internet Protokol
tj.	to je
tzn.	to znamená
tzv.	tak zvaný(á, é)
UTP	Unshielded Twisted Pair
VGA	Video Graphics Array
WiFi	Wireless Fidelity
WPA	WiFi Protected Access

Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- jsem byl seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;

- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3);

- souhlasím s tím, že bakalářská práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;

- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;

- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Havířově, dne 3. 5. 2013

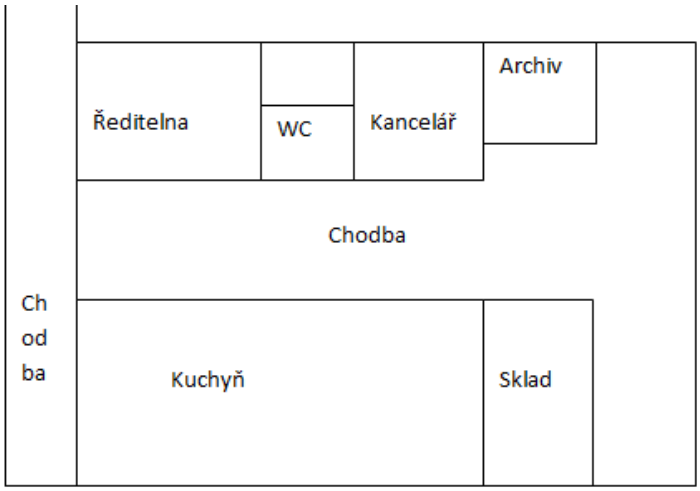
Daniel Otisk

Adresa trvalého pobytu studenta:

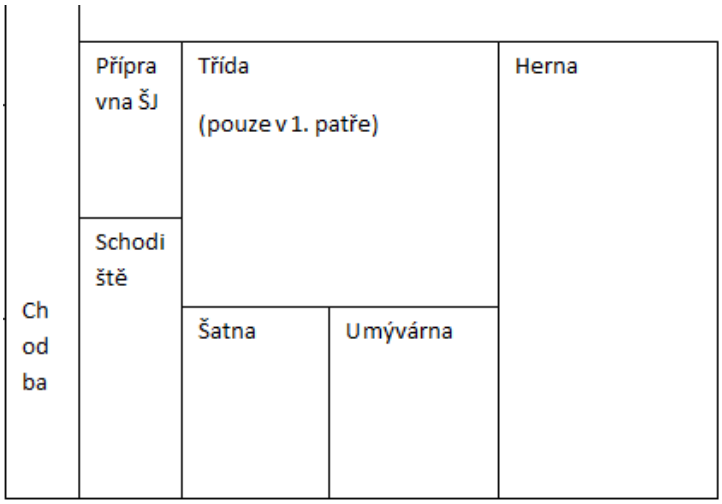
E. Urxe 1/285
736 01 Havířov-Město

Seznam příloh

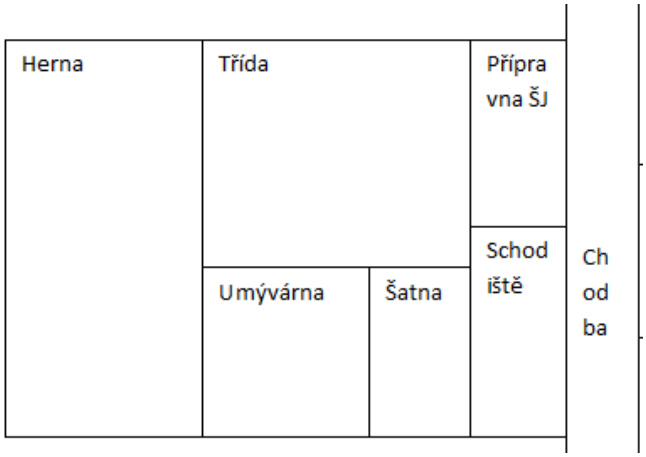
Příloha 1: Rozmístění místností na jednotlivých odděleních v budově mateřské školy



Obrázek 1: Budova A (přízemí)



Obrázek 2: Budova A (1. patro)



Obrázek 3: Budova B

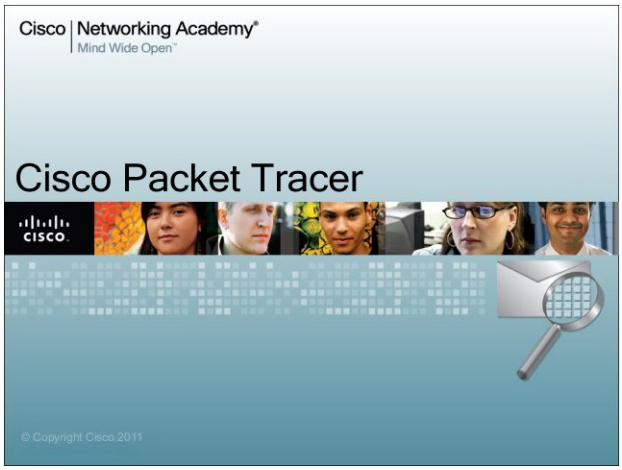
Obrázek 4: Budova C

Příloha 2: Prostředí aplikace Cisco Packet Tracer

Firma CISCO je největším světovým výrobcem síťových prvků a technologií. V tomto cenném programovém nástroji můžeme nejen vyzkoušet propojování síťových prvků a navrhování topologie sítě, ale můžeme zde přímo simulovat reálný běh aplikací s konfigurací síťových prvků a sledováním paketů mnoha síťových protokolů. Nyní si tento program stručně popíšeme. [7]

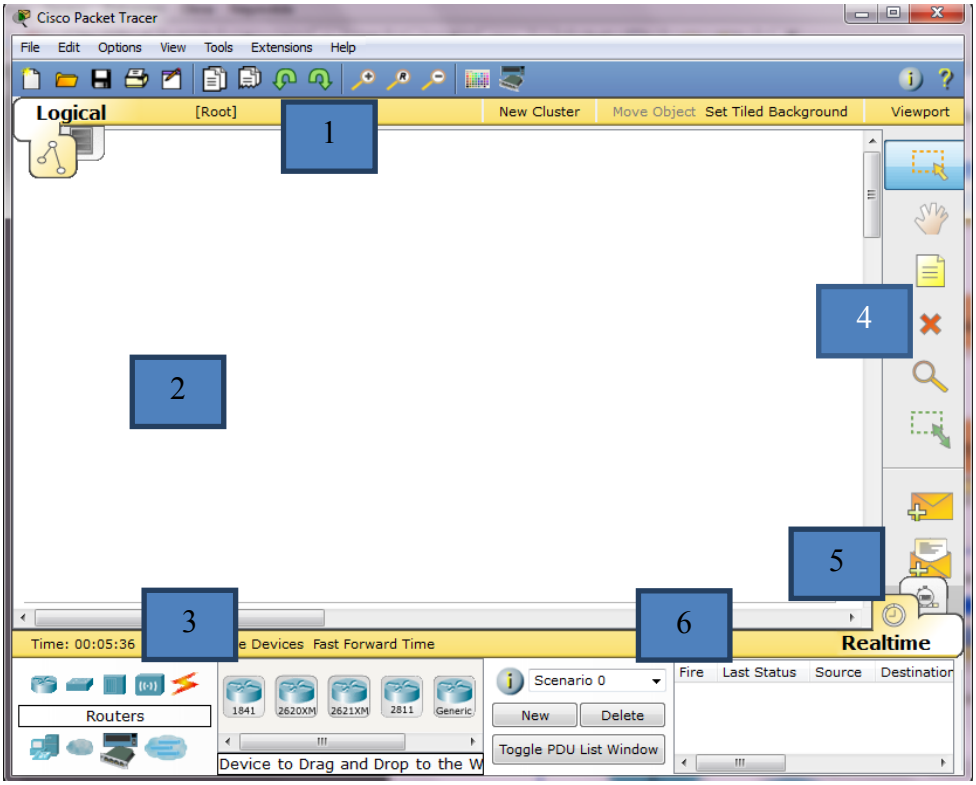
Základní popis prostředí

Program Packet Tracer nevyžaduje žádné speciální HW nároky a jeho instalace je jednoduchá. Po spuštění programu uvidíme úvodní obrazovku aplikace (viz obrázek 1) a poté se již spustí aplikace a zobrazí se pracovní plocha. [7]



Obrázek 1: Úvodní obrazovka programu

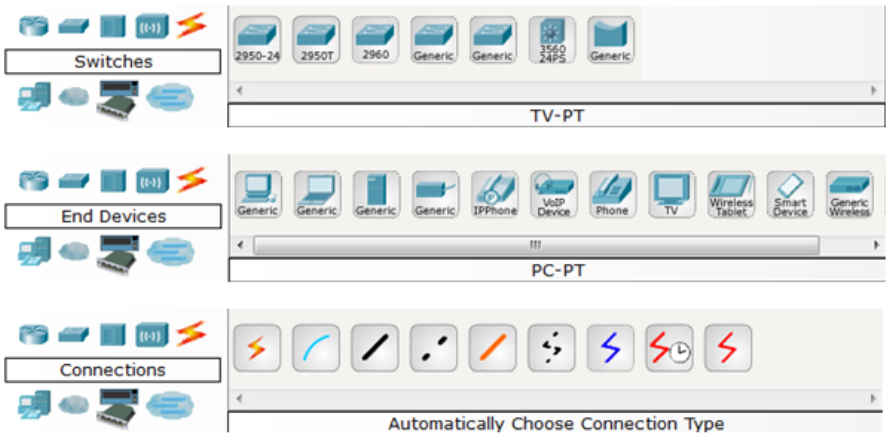
Okno aplikace je zobrazeno na obrázku 2. Při spuštění aplikace vidíme její tyto součásti: 1. Menu programu a panel rychlého spuštění, 2. Pracovní plocha aplikace, na kterou budeme vkládat všechny prvky a vytvářet topologie sítě, 3. Výběr všech dostupných síťových a koncových zařízení, 4. Panel nástrojů, 5. Přepínač reálného a simulačního módu a 6. Výběr simulačních scénářů a jejich status. [7]



Obrázek 2: Pracovní plocha programu

Vkládání prvků na pracovní plochu a jejich propojování

Ve spodní části aplikace vidíme možné síťové a koncové prvky, které můžeme vkládat na pracovní plochu. Patří mezi ně převážně routery, switche a koncová zařízení typu PC, server, tiskárna aj. Důležitým prvkem je typ propojení, viz obrázek 3 dole, kterým propojíme všechny prvky v síťové topologii. [7]



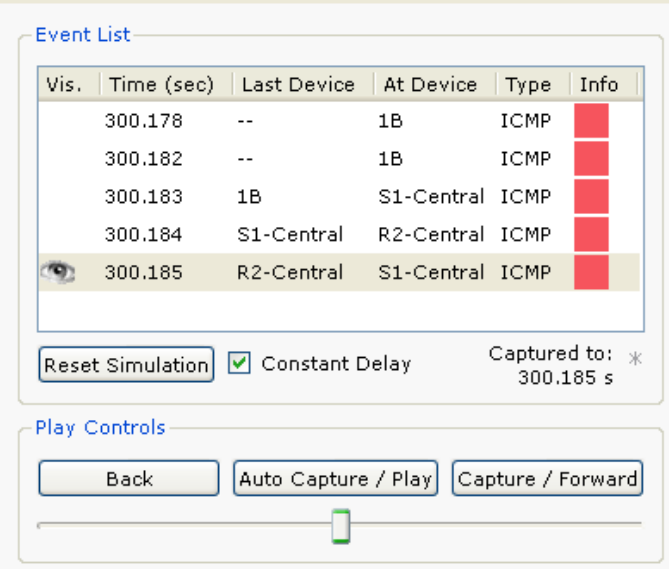
Obrázek 3: Vkládání prvků v programu

Monitorování paketů v simulačním režimu

Program Cisco Packet Tracer je mocným nástrojem, který umí simulovat běh paketů v síti. Tuto funkcionalitu zajistíme přechodem mezi real-time a simulačním módem přepínačem v pravém dolním rohu aplikace (viz. obrázek 4). [7]

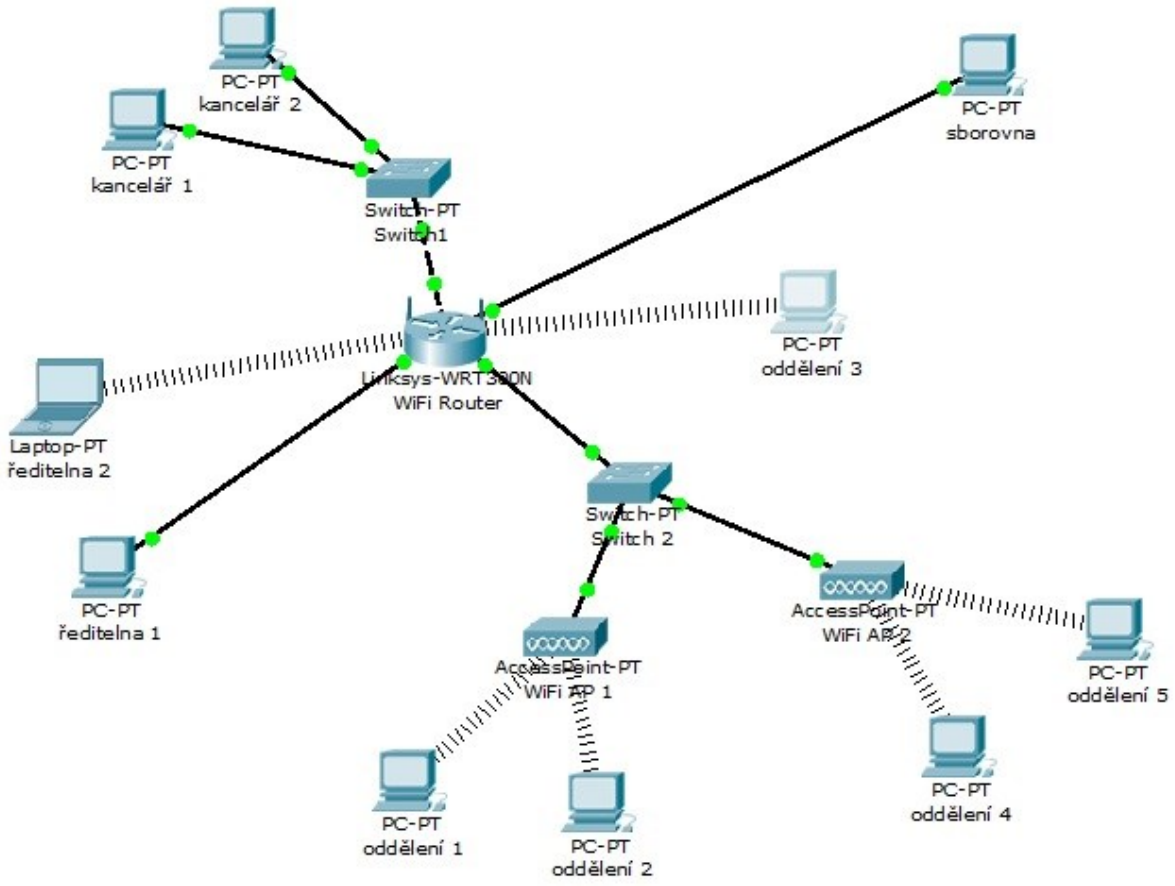
Obrázek 4: Přepínání mezi reálným a simulačním režimem

V simulačním módu můžeme ihned spustit simulaci toku paketů po síti tlačítkem Play popřípadě krokovat komunikaci tlačítkem Capture. Po spuštění simulace ať už tlačítkem Play či Capture můžeme v okně událostí Event List prohlídnout posloupnost probíhajících paketů podle filtru (viz. obrázek 5). [7]

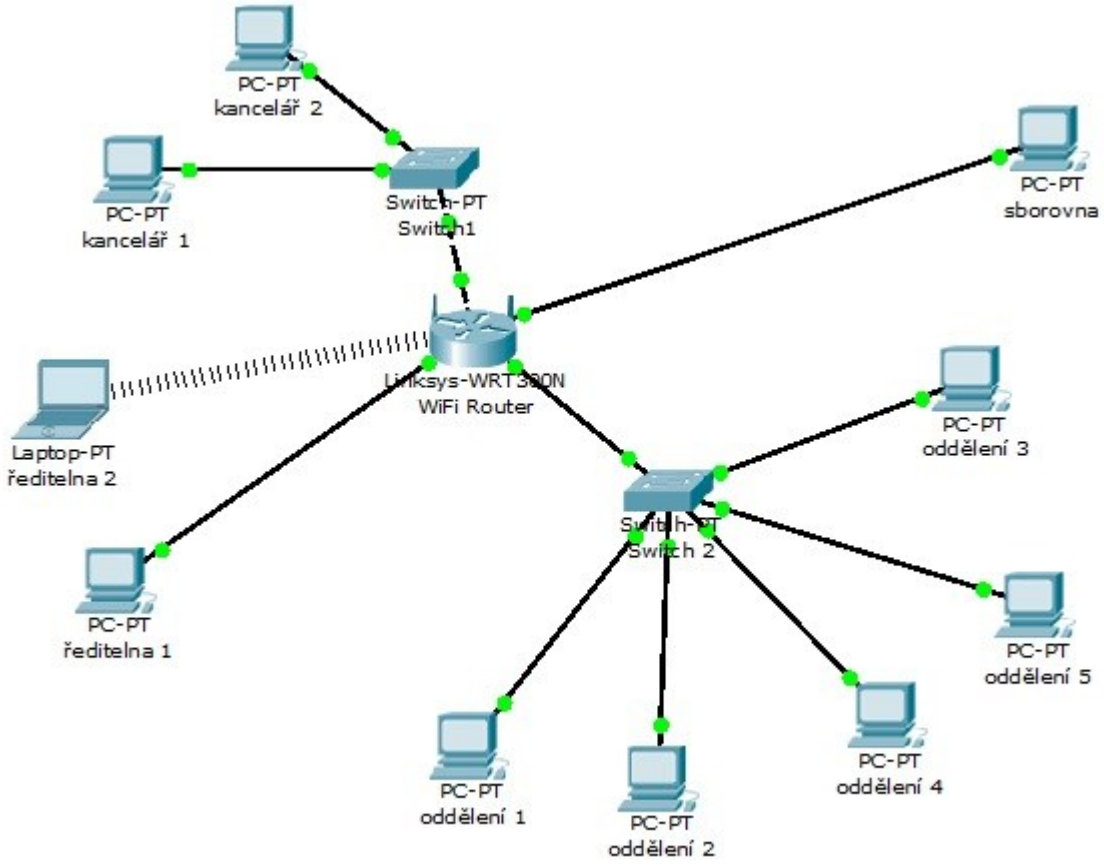


Obrázek 5: Simulace toku ICMP v náhodné síti

Příloha 3: Návrh jednotlivých variant v grafické podobě programu Packet Tracer



Obrázek 1: Návrh levnější varianty v grafickém zobrazení



Obrázek 2: Návrh dražší varianty v grafickém zobrazení